¡Soluciones!

SIESA

Para el ahorro y control de la energía eléctrica

Distribuidor autorizado:

MOXA®

MOXA VPort 3310 Industrial Video Server

User's Manual

First Edition, December 2005

MOXA

VPort 3310 User's Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Copyright © 2005 Moxa Networking Co., Ltd.
All rights reserved.
Reproduction without permission is prohibited.

Trademarks

MOXA is a registered trademark of the Moxa Group.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.

Moxa provides this document "as is," without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Moxa Networking assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Before getting started

Before using your VPort 3310, please pay close attention to the following items:

- After opening the VPort 3310 box, compare the contents of the box with the **Package Checklist in Chapter 1**. Notify your sales representative if any of the items is missing or damaged.
- To prevent damage or problems caused by improper usage, before assembling and operating the device and peripherals, read the **Quick Installation Guide** (the printed handbook included in the package). You may also refer to **Chapter 1**, under **Product Description**, and all of **Chapter 2**, of this manual.
- If you experience a system error, and the system does not recover easily, refer to the **Troubleshooting** section in **Chapter 7** to learn how to restore factory default settings and reinstall the system.
- The VPort 3310 Video Server has been designed for various environments and can be used to build various applications for general security or demonstration purposes. For standard applications, refer to **Chapter 2**, **Getting Started**, and **Chapter 3**, **Accessing VPort 3310 Video Server for the First Time**.

Important Note

- Surveillance devices may be prohibited by law in your country. Since VPort is both a high performance surveillance system and networked video server, ensure that the operations of such devices are legal in your locality before installing this unit for surveillance purposes.

Table of Contents

Chapter 1 Introduction 1-1
Overview 1-2
Package Checklist 1-3
Product Features 1-4
Typical Application 1-4
Panel Layout of VPort 3310 1-5
Product Description 1-6

Chapter 2 Getting Started 2-1
Before Getting Started 2-2
First-Time Installation and Configuration 2-2
Network Environment with a DHCP Server 2-3
Network Environment without a DHCP Server 2-5
Mounting VPort 3310 2-8
Mounting Dimensions 2-8
DIN-Rail Mounting 2-9
Wall Mounting (Optional) 2-9
Wiring Requirements 2-10
Grounding MOXA VPort 3310 2-11
Wiring the Relay Contact 2-11
Wiring the Redundant Power Inputs 2-11
Wiring the Digital Inputs 2-12
10/100BaseT(X) Ethernet Port Connection 2-12

Chapter 3 Accessing VPort 3310's Web-based Manager 3-1
Functions Featured on VPort's Homepage 3-2
Logo and Host Name 3-2
Camera Image View 3-2
Video Information 3-2
Client Settings 3-2
System Configuration 3-3
Video/Audio Control by Clients 3-3
Video Image Snapshots 3-4
DI Status/Relay Control 3-4
Motorized (PTZ) Camera Control 3-4
Custom PTZ Camera Commands 3-4

Chapter 4 System Configuration 4-1
System Configuration via Web-based Manager 4-2
VPort Video Server Information 4-3
System 4-3
Network 4-9
Video 4-23
Audio 4-30
Alarm 4-30
System Configuration via FTP 4-38
Parameters Available in Config.ini 4-38

Chapter 5 URL (CGI) Commands 5-1
Overview 5-2
Style Convention 5-2

General CGI URL Syntax and Parameters 5-2
Get Server Parameter Values 5-3
Set Server Parameter Values 5-3
Drive the Digital (Relay) Output 5-4
Query Status of the Digital Input 5-5
Query Status of the Digital (Relay) Output 5-5
Capture Single Snapshot 5-6
Account Management 5-6
System Logs 5-7
Configuration File 5-8
Camera Control 5-8
Recall 5-8
System Information 5-9
Preset Locations 5-11

Appendix A Frequently Asked Questions A-1

Appendix B Settings of Supported PTZ Cameras B-1

Appendix C Time Zone Table C-1

Appendix D Technical Specifications D-1

Appendix E Service Information E-1

MOXA Internet Services E-2
Problem Report Form E-3
Product Return Procedure E-4

1

Introduction

VPort 3310 is a high-performance networking video server. In addition to being able to handle basic video feed, many advanced features are also included to set up surveillance or web attraction applications. VPort 3310 is designed to provide stability, robustness, ease-of-use, and flexibility.

The following topics are covered in this chapter:

- **Overview**
- **Package Checklist**
- **Product Features**
- **Typical Application**
- **Panel Layout of VPort 3310**
- **Product Description**

Overview

VPort 3310 is a 1-channel Industrial Video Server that uses the standard MPEG4 algorithm, and features DIN-Rail Mounting capability, 24 VDC redundant power inputs, and IP30 protection to meet the requirements of industrial environments. VPort 3310 can digitize any analog video source and distribute these digital images over an IP network, turning your CCTV system into a "Video over IP" Network System INSTANTLY. The cutting edge MPEG4 algorithm gives VPort 3310 an FPS of up to 30 in CIF resolution (352 x 240), with maximum bandwidth of 1.6 Mbps, to provide high video performance and more efficient network transmission. In addition, VPort 3310 also provides audio communication for a voice over IP solution, making the control of your video surveillance system more real-time.

In addition, VPort 3310-T is rated to operate at temperatures ranging from -40 to 75°C, which is especially suitable for outdoor applications.

High Performance MPEG4 compression
Video input can be efficiently compressed into MPEG4 video stream packets without delay. This is all done without sacrificing remote monitoring capability or storage. Five levels of compression ratio and three different image resolutions are provided to provide more versatility.

Audio supported for a complete surveillance solution
The MPEGx series algorithm allows both voice and video to be compressed together to provide users with more versatile applications, such as VCD (MPEG1), DVD (MPEG2), Internet Multimedia Broadcast (MPEG4), etc. VPort 3310 introduces users to a brand new kind of synchronized video/audio surveillance over an IP network.

Rugged Design for Industrial Environments
VPort 3310 is an Industrial Video Server, which means that it is specially design for harsh industrial environments. With the 24 VDC redundant power inputs, IP30 protection, and DIN-Rail mounting, VPort 3310 meets the critical requirements of most industrial applications. Most importantly, VPort 3310-T can operate reliably in a -40 to 75°C temperature range, making it the first video server of its kind that can be used for extended temperature, industrial-grade applications. VPort 3310-T is an optimal solution for outdoor environments.

RTSP Streaming for Easy Integration
RTSP (Real-time Streaming Protocol) is a client-server multimedia presentation control protocol, which enables the interoperability of video devices and software. Hardware or software that supports RTSP streaming can easily identify and decode the video stream without the hassle of codec installation. For example, users can view video images from VPort 3310 directly with Quick Time and Real Player, both of which support RTSP streaming.

Multicast (IGMP) Transmission for Network Efficiency
Transmitting digital video images via an IP network requires a dozen times the bandwidth compared to general data. For this reason, the efficiency of network bandwidth management is one of the most important issues that determines the performance of a video over IP surveillance system. VPort 3310 supports multicast transmission with IGMP protocol, which can reduce the bandwidth requirements when multiple clients access the same video stream, and greatly increases the efficiency of network bandwidth management.

PPPoE for Easy xDSL Connections
xDSL is one of the most popular Internet media in the world today. VPort 3310 supports the PPPoE protocol to make it easier to connect to an xDSL connection. In fact, VPort 3310 can build an xDSL connection with an ISP directly without using an xDSL router.

SNMP for Network Management Systems
SNMP is the most popular network management protocol due to it interoperability and ease-of-use. Most network devices support the SNMP protocol, as does most system software. VPort 3310 supports SNMP V1, V2c, and V3 to make it easier to integrate with the network management system.

Easy Web access via standard browsers
There is no need to install new software to access the Video Server, since the embedded Web Server allows users to use any popular web browser to access the Video Server from anywhere over the Internet. As long as you are connected to the network, you will be able to view the same images seen by your cameras.

Built-in 3 area-selectable Video Motion Detection (VMD)
External sensors are not required, since the video channel can be configured to detect motion in 3 areas, making it easy to set up a security system in either your office or the field. And the customizable settings allow you to tune the system for both object size and sensitivity, making the Video Server adaptable to different environments.

Weekly schedule for automated surveillance
The user-defined time period will check security settings on a weekly basis, and send notifications or drive external devices, making VPort 3310 suitable for more versatile applications.

Flexible I/O control for external devices
One opto-isolated sensor input and one relay output are provided to control external devices, giving system integrators the option of turning an analog system into an advanced security system.

MOXA SoftDVR Lite IP Surveillance Software
To extend the Video Server's capabilities, MOXA SoftDVR™ Lite IP Surveillance Software, which supports a maximum of 4 cameras in quad, is included free of charge, allowing users to turn their PC into a digital video recorder. Scheduling or one-click recording saves important images on your local hard disk, and the reliable motion detection and instant warning features make you ready for any situation. A quick and easy to use search and playback function lets you easily find the image you're looking for, so that you can inspect the images more carefully, and also save the output to an AVI file.

SDK support for developers
The high-performance Video Server can be integrated into many applications—without busting your budget—and the complete programming interface of MOXA ActiveX Control SDK and C library API SDK make the developer's job easy and straightforward. To ask about SDK requirements, please contact a MOXA Sales representative for details and an application form.

Package Checklist

MOXA VPort 3310 is shipped with the following items. If any of these items is missing or damaged, please contact your customer service representative for assistance.

- VPort 3310 or VPort 3310-T x 1
- 6-pin terminal block x 2 for power inputs, DIs, and relays
- 2-pin terminal block x 1 for RS-485 connection
- Quick Installation Guide
- Software CD with User's Manual, Quick Installation Guide, MOXA DVN Solution Datasheet, SoftDVR Lite IP Surveillance Software, IP Reporter, and MIB file
- Warranty booklet

NOTE: Notify your sales representative if any of the above items is missing or damaged.

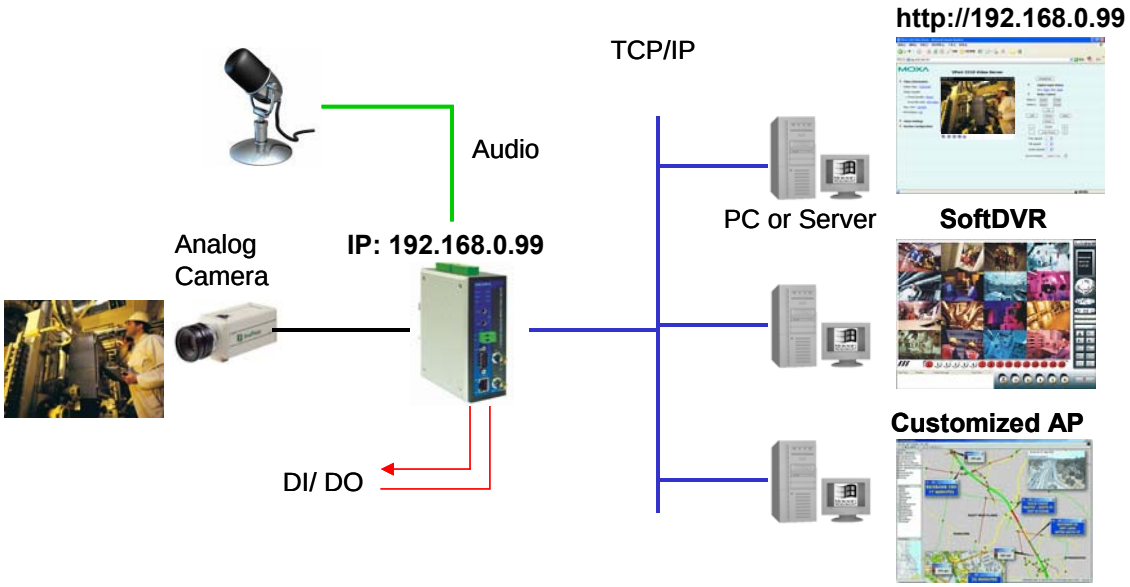
Product Features

VPort 3310 has the following features:

- Digitizes analog video signals INSTANTLY
- 1-ch video input and 1-ch video output
- Audio supported for synchronal video/audio surveillance solution
- Remote access with built-in web server for viewing and configuring
- Optimal solution by adjustable frame rate, bandwidth, and quality
- RTSP video streaming
- Built-in 3 area selectable Video Motion Detection (VMD)
- Video stream up to 30 frames/sec at a resolution of 352 x 240
- Effective traffic control with Multicast (IGMP)
- SNMP MIB-II for network management
- Redundant 24 VDC power inputs and power failure alarm
- PTZ (PAN/TILT/ZOOM) motorized camera control via RS-232/RS-485 COM port
- Equipped with 2 DIs and 2 Relays for external sensors and alarms
- PPPoE and DDNS supported for the convenience of xDSL connection
- IP30 protection form factor
- Optional -40 to 75°C operating temperature
- Remotely upgrade the firmware to keep it up to date
- MOXA SoftDVR™ IP Surveillance Software for viewing and recording bundled free

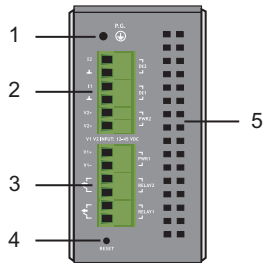
NOTE: ActiveX Control SDK supports a flexible interface and sample codes for third-party developers (contact a Moxa sales representative for more information about this SDK).

Typical Application

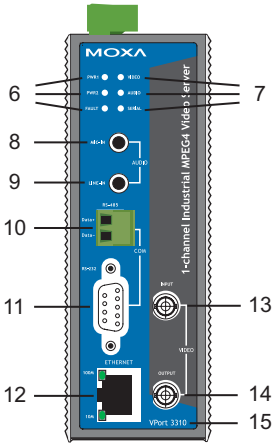


Panel Layout of VPort 3310

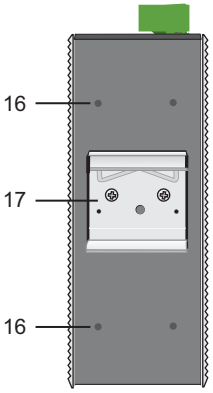
Top Panel View



Front Panel View



Rear Panel View



1. Grounding screw
2. 6-pin terminal block for DI 1, DI 2, power input 2 (PWR2)
3. 6-pin terminal block for Relay 1, Relay 2, power input 1 (PWR1)
4. Hardware reset button
5. Heat dissipation orifices
6. LEDs for PWR1, PWR2, FAULT
7. LEDs for VIDEO, AUDIO, SERIAL
8. MIC-IN audio input port
9. LINE-IN audio input port
10. 2-pin terminal block for RS-485 connection
11. DB9 port for RS-232 connection
12. RJ45 Ethernet Port with 10 Mbps, 100 Mbps LEDs
13. BNC port for video input
14. BNC port for loop-through video output
15. Model name
16. Screw hole for wall mounting kit
17. DIN-Rail mounting kit

Product Description

BNC video input/output

The BNC video input is a 75 Ohm video port for connecting an external camera. To ensure that the correct video modulation type is detected, cameras should be connected and powered on before the VPort is powered on.

Phone jack audio input

There are 2 phone jack audio inputs on the front panel. One is for MIC-in connection, which can be directly connected with a microphone; the other is for Line-in connection, which can be connected with an audio source from an amplifier.

LED Indicators

The front panel of MOXA VPort 3310 contains several LED indicators. The function of each LED is described in the table below.

LED	Color	State	Description
PWR1	AMBER	On	Power is being supplied to power input PWR1
		Off	Power is **not** being supplied to power input PWR1
PWR2	AMBER	On	Power is being supplied to power input PWR2
		Off	Power is **not** being supplied to power input PWR2
FAULT	RED	On	One of the 2 power inputs is disconnected or does not work properly
		Off	Both power inputs are connected and working properly
VIDEO	GREEN	On	Video signal has been detected
		Off	Video signal has not been detected
AUDIO	GREEN	On	Audio signal has been detected
		Off	Audio signal has not been detected
SERIAL	GREEN	On	RS-232 or RS-485 signals are being transmitted
		Off	RS-232 or RS-485 signals are not being transmitted or have not been detected

10/100 Mbps Ethernet port

Use a UTP CAT5 cable shorter than 100 meters to connect VPort 3310 to an Ethernet network. There are 2 LED indicators at the corner of the RJ45 Ethernet port. The main purpose of the LED indicators is to show if the link speed is 10 Mbps or 100 Mbps.

NOTE After powering on the VPort 3310, wait a few seconds for the POST (Power On Self Test) to run. When the POST is running, the AUDIO and SERIAL LED will blink in sequence a few times. The IP address will be assigned when the 10 or 100 Mbps NETWORK LED blinks.

RS-232/RS-485 COM port

VPort 3310 provides 1 COM port for PTZ control. However, two ports are available to connect an external controller to VPort 3310's PTZ COM port. One port is a male DB9 port for RS-232 signals, and the other port is a 2-pin terminal block for RS-485 signals.

NOTE Since RS-485 port and RS-232 port share the same UART chip, your may use either the RS-485 port, or the RS-232 port, but not both.

Redundant 24 VDC power inputs

VPort 3310 has two power inputs to provide redundancy. The 24 VDC power input is used mostly in industrial environments. You should check the LED indicators to see if the power inputs are working properly.

General I/O terminal blocks

Two 6-pin terminal block connectors located on VPort 3310's top panel are for connecting the 24 VDC power source and GPIO. VPort 3310 provides 2 digital inputs and 2 relay outputs for linking to peripheral devices, such as sensors and alarms. These I/O connections can be employed when using VPort 3310 to create an intelligent alarm system for system operation (power failure, video loss, disconnected network) or triggered event (VMD).

Relay Output		Normal Open	Max. 1A, 24 VDC
		Normal Close	Initial status is Normal Open
Digital Input	⊥	DI-	"High": +13V to +30V
	I1, I2	DI+	"Low": -30V to +3V

NOTE Please refer to VPort 3310's Quick Installation Guide to see how to wire the digital inputs and relay outputs.

Reset Button

A recessed RESET button is provided for restoring the system to the factory default settings. When the system fails to install properly, or operates abnormally, push the RESET button located on the top panel of VPort 3310 to restore the factory defaults. The following steps explain how to use the RESET button:

Step 1: Prepare a thin stick, such as a toothpick or paperclip, to push the reset button.

Step 2: Depress the reset button until the AUDIO and SERIAL LEDs flash in sequence 5 times.

Step 3: Remove the thin stick from the RESET button. The server will run the POST process to reboot.

Step 4: Either the 10M LED or 100M LED will illuminate when the system has finished rebooting.

2

Getting Started

This chapter includes information about how to install a VPort 3310 Video Server.

The following topics are covered:

- **Before Getting Started**
- **First-Time Installation and Configuration**
  - Network Environment with a DHCP Server
  - Network Environment without a DHCP Server
- **Mounting VPort 3310**
  - Mounting Dimensions
  - DIN-Rail Mounting
  - Wall Mounting (Optional)
- **Wiring Requirements**
  - Grounding MOXA VPort 3310
  - Wiring the Relay Contact
  - Wiring the Redundant Power Inputs
  - Wiring the Digital Inputs
  - 10/100BaseT(X) Ethernet Port Connection

Before Getting Started

In what follows, "user" refers to those who can access the Video Server, and "administrator" refers to the person who knows the root password that allows changes to the Video Server's configuration, in addition to providing general access. Administrators should read this part of the manual carefully, especially during installation.

First-Time Installation and Configuration

Before installing VPort 3310, check to make sure that all items in the Package Checklist are in the box. In addition, you will need access to a notebook computer or PC equipped with an Ethernet port.

Step 1: Select the Power Source

VPort 3310 can be powered by a DC power input from 12 to 45 VDC. Two power inputs are provided for redundancy. Users can check the LED status located in the front panel to see if the power inputs are connected appropriately. If one of the power inputs fails, the FAULT LED will illuminate in red.

Step 2: Connect VPort 3310 to a Network

VPort 3310 provides auto-sensing 10/100 Mbps network connectivity. Each RJ45 Ethernet port has 2 LEDs. One LED is used to indicate if the 10 Mbps connection is active, and the other LED is used to indicate if the 100 Mbps connection is active.

Step 3: Connect VPort 3310 to a camera and an audio source

VPort 3310 supports a **VIDEO INPUT** port and a loop-through **VIDEO OUTPUT** port. Users should use the BNC connector and coaxial cable to connect the video camera with VPort to input the analog video signals, and connect the monitor or DVR with VPort to output analog signals.

VPort 3310 provides 2 audio inputs for the audio source. A microphone can be plugged directly into the **MIC-IN** port; an amplifier can be plugged into the **LINE-IN** port.

NOTE **VIDEO** and **AUDIO** LEDs are located on the front panel to indicate the signal transmission status for video and audio input. Users can check the LED status to see if the video and audio are in proper working order.

Step 4: Connecting VPort 3310 with a motorized PTZ Camera/Device

If a PTZ camera or device is used, users need to connect the PTZ control cable to VPort 3310's COM port. VPort 3310 has 2 serial ports. One is an RS-232 DB9 port, and the other is an RS-485 2-pin terminal block port. However, the two ports cannot be used simultaneously. To enable PTZ control, users should configure the PTZ control protocol in the web-based manager.

NOTE The PTZ control protocol is not standardized. To use a particular PTZ control protocol, the video server must support the driver for that protocol. Currently, VPort 3310 supports PTZ control protocol drivers for:

1. Sony VISCA
2. Cannon VC-C1/ VC-C3/ VC-C4
3. Samsung SmartDome
4. Pelco D
5. DynaColor SmartDome
6. Liling PIH-7x00
7. Ernitec

VPort 3310 can be used to control PTZ cameras that support these PTZ protocols. If you need to use a protocol that is not on the list, you will need to contact the manufacturer of the camera to get the PTZ control commands, and then program VPort 3310's **Custom Camera** function.

Step 5: Configure VPort 3310's IP address

After powering on the VPort 3310, wait a few seconds for the POST (Power On Self Test) to run. When the POST is running, the AUDIO and SERIAL LED will blink in sequence a few times. The IP address will be assigned when the 10 or 100 Mbps NETWORK LED blinks. The IP address assigned after the POST is completed will be based on the network environment.

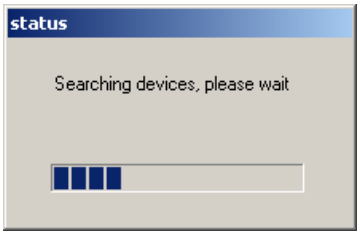
Network Environment with a DHCP Server

When VPort 3310 is configured for DHCP, VPort 3310's IP address will be assigned by a DHCP Server. Use the DHCP Server's IP address table, or use the MOXA IP Reporter utility to determine the IP address that was assigned by the DHCP Server.

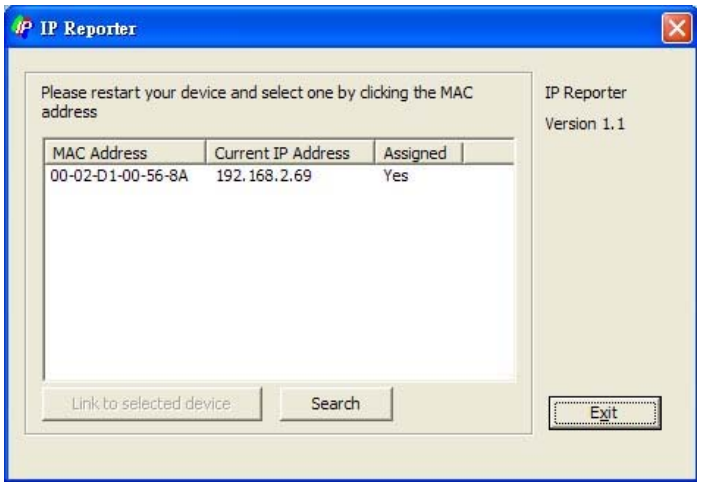
NOTE After powering on the VPort 3310, wait a few seconds for the POST (Power On Self Test) to run. When the POST is running, the AUDIO and SERIAL LED will blink in sequence a few times. The IP address will be assigned when the 10 or 100 Mbps NETWORK LED blinks.

Using IP Reporter

1. Run the **IPReporter.exe** program to search for the VPort. After the IP Reporter window opens, you may also click on the **Search** button to initiate a search.

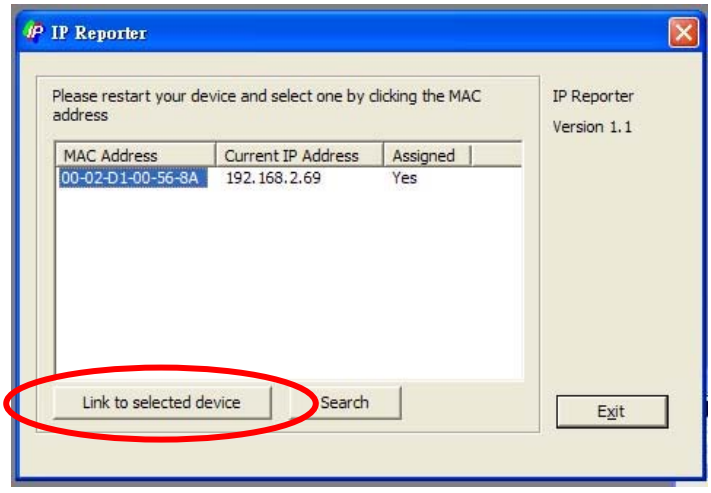


2. When the search has concluded, the MAC address and IP address of the VPort will be listed in the IP Reporter window.



NOTE The **Assigned** status will be listed as **Yes** if the VPort has been assigned an IP address. If the DHCP installation function is supported, check to see if there are any problems with the network environment.

3. Click on the VPort whose MAC address matches the one you just installed, and then click on **Link to the selected device** to access the VPort via your web browser. You will be able to modify VPort's IP address and other settings when the VPort's homepage opens.



Network Environment without a DHCP Server

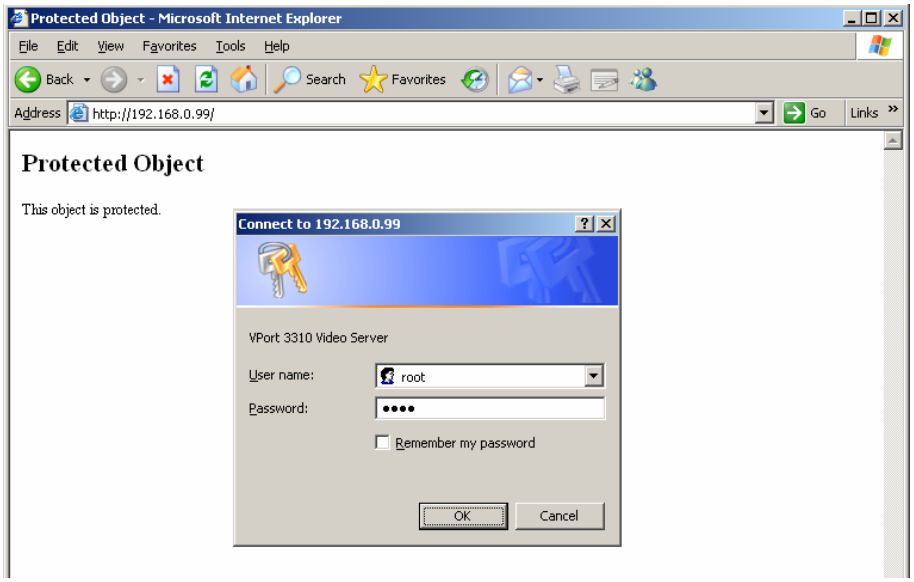
If your VPort 3310 is connected to a network that does not have a DHCP server, then you will need to configure the IP address manually. There are two ways to access the server:

1. If one VPort 3310 is connected to the network, open your web browser and type the default IP address in the browser's address box. In this case, the default IP address is **192.168.0.99** and the default subnet mask is **255.255.255.0**. Note that you may need to change your computer's IP address and subnet mask so that the computer is on the same subnet as the VPort.
2. If VPort 3310 detects that another host on the network has already been assigned IP address 192.168.0.99, then the VPort 3310 will use the next available IP (192.168.0.100, or 192.168.0.101, etc.) as its default IP address. In this case, you can use Moxa's IP Reporter utility to locate each VPort connected to the network. Since IP Reporter searches by MAC address, the VPort and computer just need to be connected to the same Ethernet LAN for IP Reporter to locate the VPort.

To change the IP address of VPort manually, access VPort's web server, and then navigate to the **System Configuration → Network → General** page to configure the IP address and other network settings. Check the **Use fixed IP address** to ensure that the IP address you assign is not deleted each time the VPort is restarted.

Step 6: Authentication for Accessing VPort 3310 Web-based Manager

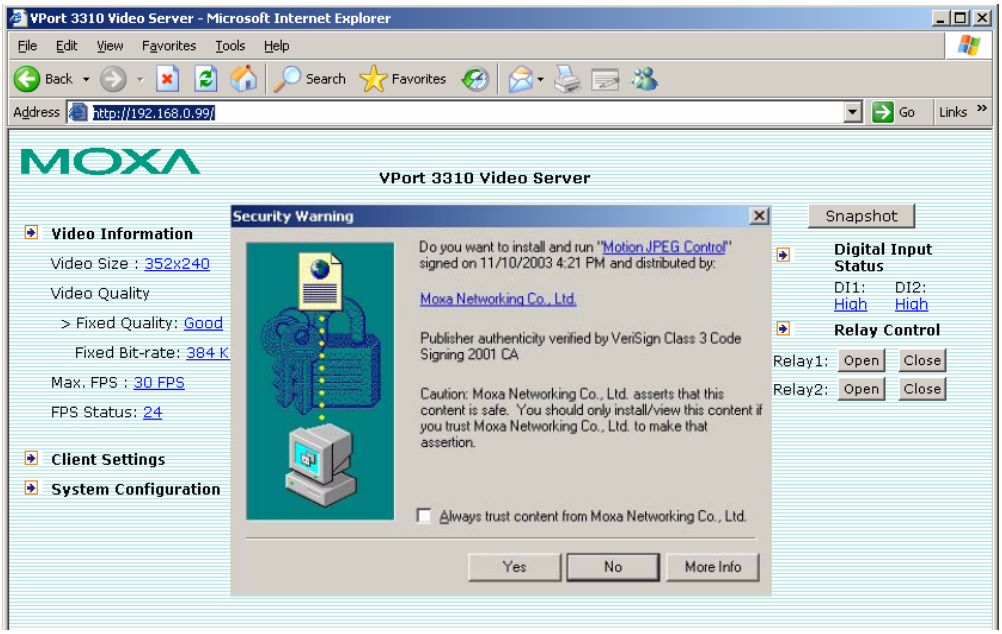
1. Type the IP address in the web browser's address input box and then press enter.
2. A window will open asking you to enter the user name and password for authentication. For first time access, the administrator must type **root** for user name, and **root** for password. Click on **OK** to continue.



After entering the VPort configuration main page, the administrator can configure different user names and passwords so that different users can access the same VPort..

Step 7: Installing the ActiveX Control Plug-in

A security warning message will appear the first time you access VPort's web-based manager. The message is related to installing the VPort AcitveX Control component to your PC or notebook. Click on Yes to install this plug-in to enable the IE web browser for viewing video images.

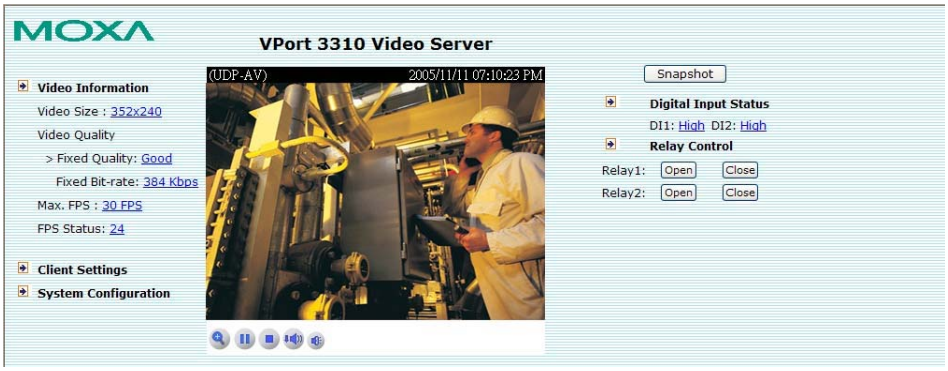

VPort 3310 Video Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.0.99/
Go Links
MOXA
VPort 3310 Video Server
Video Information
Video Size : 352x240
Video Quality
> Fixed Quality: Good
Fixed Bit-rate: 384 K
Max. FPS : 30 FPS
FPS Status: 24
Client Settings
System Configuration
Security Warning
Do you want to install and run "Motion JPEG Control" signed on 11/10/2003 4:21 PM and distributed by:
Moxa Networking Co., Ltd.
Publisher authenticity verified by VeriSign Class 3 Code Signing 2001 CA
Caution: Moxa Networking Co., Ltd. asserts that this content is safe. You should only install/view this content if you trust Moxa Networking Co., Ltd. to make that assertion.
Always trust content from Moxa Networking Co., Ltd.
Yes
No
More Info
Snapshot
Digital Input Status
DI1: High DI2: High
Relay Control
Relay1: Open Close
Relay2: Open Close

NOTE For Windows XP SP2 or above, the ActiveX Control component will be blocked for system security reasons. In this case, VPort's security warning message window may not appear. Users should unlock the ActiveX control blocked function or disable the security configuration to enable the installation of VPort's ActiveX Control component.

Step 8: Accessing the Homepage of VPort 3310's Web-based Manager

After installing the ActiveX Control component, the homepage of VPort 3310's web-based manager will appear. Check the following items to make sure the system was installed properly:

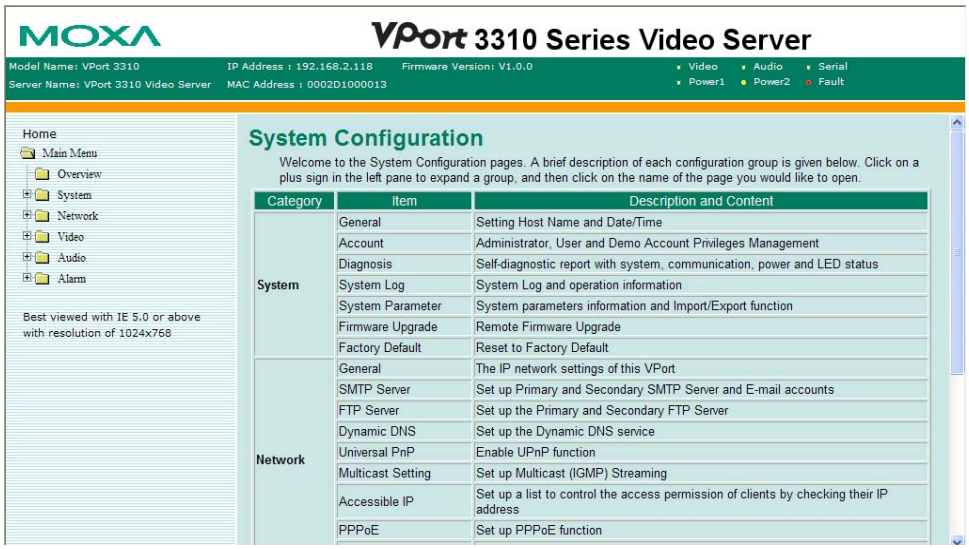
1. Video Images
2. Audio Sound (make sure your PC's or notebook's sound is turned on)
3. Video Information



Step 9: Accessing VPort's System Configuration

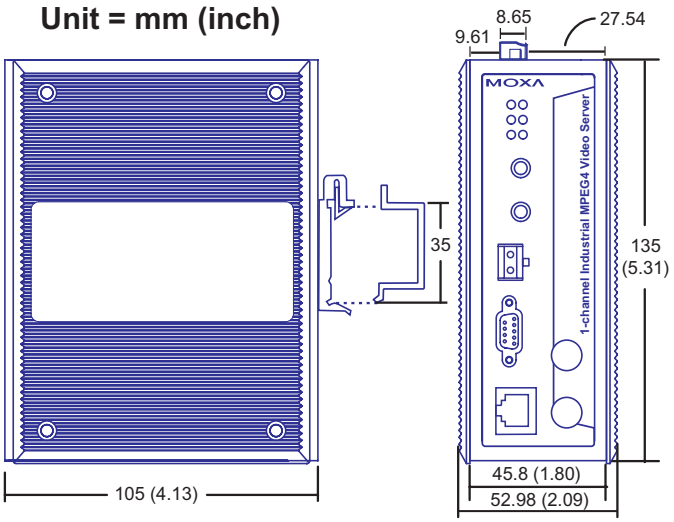
Click on **System Configuration** to access the overview of the system configuration to change the configuration. **Model Name**, **Server Name**, **IP Address**, **MAC Address**, **Firmware Version**, and **LED Status** appear in the green bar near the top of the page. Use this information to check the system information and installation.

Details of each configuration are described in this User's Manual.

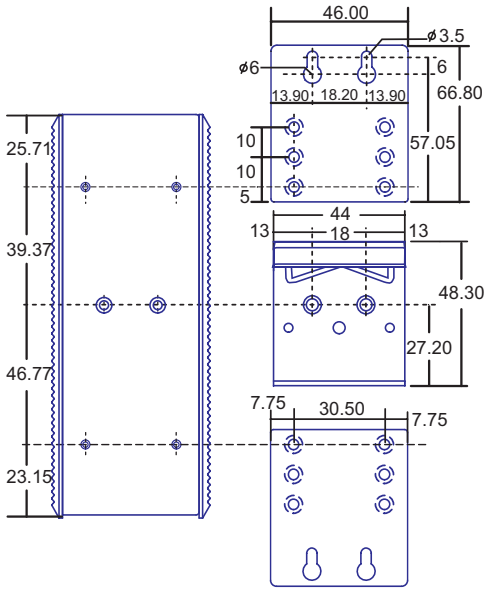


Mounting VPort 3310

Mounting Dimensions



Side View DIN-Rail Kit Front View

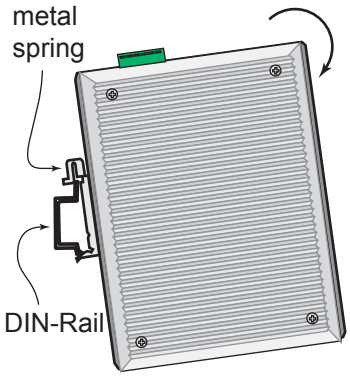


Rear View Panel Mounting Kit

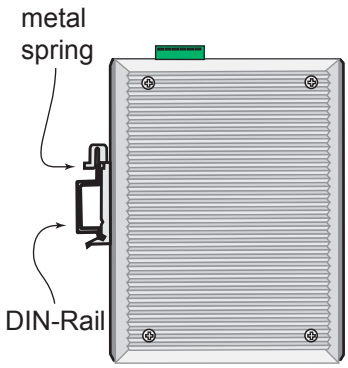
DIN-Rail Mounting

The aluminum DIN-Rail attachment plate should already be attached to the back panel of VPort 3310 when you take it out of the box. If you need to reattach the DIN-Rail attachment plate to VPort 3310, make sure the stiff metal spring is situated towards the top, as shown in the figures below.

STEP 1:
Insert the top of the DIN-Rail into the slot just below the stiff metal spring.



STEP 2:
The DIN-Rail attachment unit will snap into place as shown below.

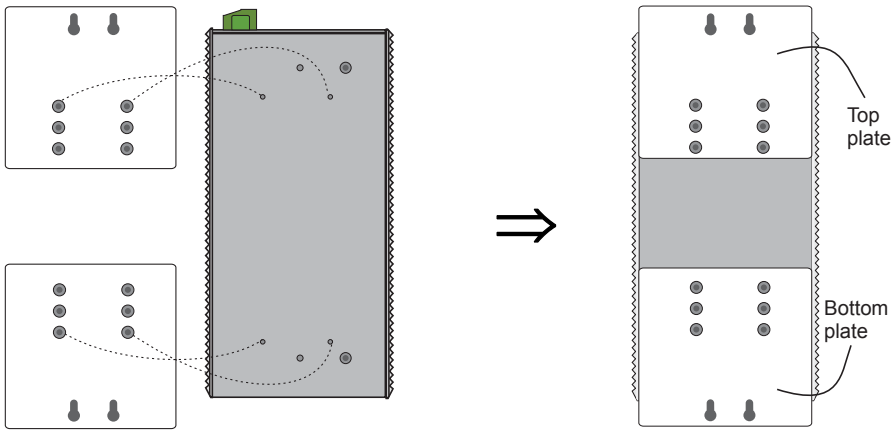


To remove VPort 3310 from the DIN-Rail, simply reverse Steps 1 and 2 above.

Wall Mounting (Optional)

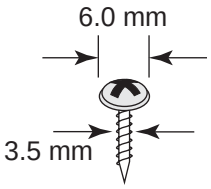
For some applications, you will find it convenient to mount VPort 3310 on the wall, as illustrated below.

STEP 1:
Remove the aluminum DIN-Rail attachment plate from VPort 3310, and then attach the wall mounting plates, as shown in the diagrams below.



STEP 2:

Mounting VPort 3310 on the wall requires 4 screws. Use the VPort 3310, with wall mounting plates attached, as a guide to mark the correct locations of the 4 screws. The heads of the screws should be less than 6.0 mm in diameter, and the shafts should be less than 3.5 mm in diameter, as shown in the figure at the right.

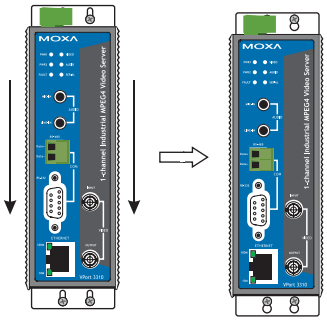


Do not screw the screws in all the way—leave a space of about 2 mm to allow room for sliding the wall mounting plates between the wall and the screws.

NOTE Test the screw head and shank size by inserting the screw into one of the keyhole shaped apertures of the Wall Mounting Plates, before it is screwed into the wall.

STEP 3:

Once the screws are fixed in the wall, insert the four screw heads through the large parts of the keyhole-shaped apertures, and then slide VPort 3310 downwards, as indicated below. Tighten the four screws for added stability.



Wiring Requirements

ATTENTION

Safety First!

Be sure to disconnect the power cord before installing and/or wiring your MOXA VPort 3310.

Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size.

If the current goes above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.

You should also pay attention to the following:

- Use separate paths to route wiring for power and devices. If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the intersection point.

  NOTE: Do not run signal or communications wiring and power wiring in the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.
- You can use the type of signal transmitted through a wire to determine which wires should be kept separate. The rule of thumb is that wiring that shares similar electrical characteristics can be bundled together.
- Keep input wiring and output wiring separated.
- It is strongly advised that you label wiring to all devices in the system when necessary.

Grounding MOXA VPort 3310

Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the ground screw to the grounding surface prior to connecting devices.

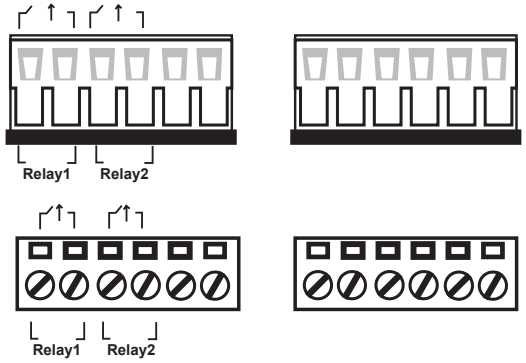
ATTENTION

This product is intended to be mounted to a well-grounded mounting surface such as a metal panel.

Wiring the Relay Contact

VPor 3310 has two sets of relay output—relay 1 and relay 2. Each Relay Contact consists of the two contacts of the terminal block on VPort 3310's top panel. Refer to the next section for detailed instructions on how to connect the wires to the terminal block connector, and how to attach the terminal block connector to the terminal block receptor.

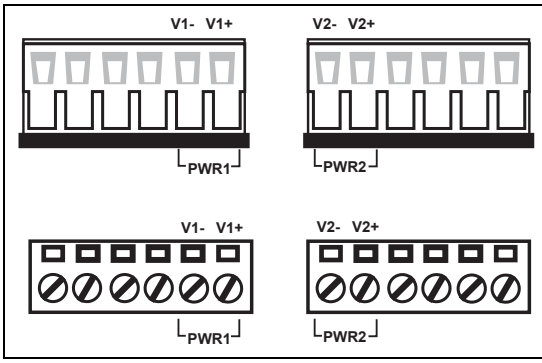
In this section, we will explain the meaning of the two contacts used to connect the Relay Contact.



FAULT:
The two sets of relay contacts of the 6-pin terminal block connector are used to detect user-configured events. The two wires attached to the Fault contacts form an open circuit when a user-configured event is triggered. If a user-configured event does not occur, the Fault circuit will be closed.

Wiring the Redundant Power Inputs

VPort 3310 has two sets of power input—power input 1 and power input 2.The top two contacts and the bottom two contacts of the 6-pin terminal block connector on VPort's top panel are used for VPort's two digital inputs. Top and front views of one of the terminal block connectors are shown here.



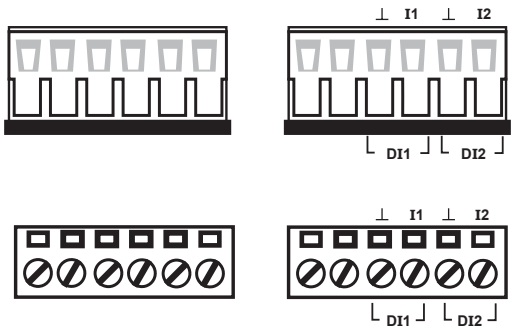
STEP 1: Insert the negative/positive DC wires into the V-/V+ terminals.

STEP 2: To keep the DC wires from pulling loose, use a small flat-blade screwdriver to tighten the wire-clamp screws on the front of the terminal block connector.

STEP 3: Insert the plastic terminal block connector prongs into the terminal block receptor, which is located on VPort 3310's top panel.

Wiring the Digital Inputs

VPort 3310 has two sets of digital input, DI 1 and DI 2. Each DI consists of two contacts of the 6-pin terminal block connector on VPort's top panel, which are used for VPort's two DC inputs. Top and front views of one of the terminal block connectors are shown here.



STEP 1: Insert the negative (ground)/positive DI wires into the ⊥/I1 terminals.

STEP 2: To keep the DI wires from pulling loose, use a small flat-blade screwdriver to tighten the wire-clamp screws on the front of the terminal block connector.

STEP 3: Insert the plastic terminal block connector prongs into the terminal block receptor, which is located on VPort 3310's top panel.

10/100BaseT(X) Ethernet Port Connection

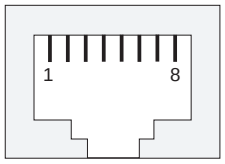
The 10/100BaseT(X) port located on VPort 3310's front panel is used to connect to Ethernet-enabled devices.

Below we show pinouts for both MDI (NIC-type) and MDI-X (HUB/Switch-type) ports, and also show cable wiring diagrams for straight-through and cross-over Ethernet cables.

The 10/100BaseT(X) port of VPort 3310 is an MDI port, which means you should use a cross-over Ethernet cable to connect to the MDI NIC port, and a straight-through Ethernet cable to connect to the MDI-X HUB/Switch port.

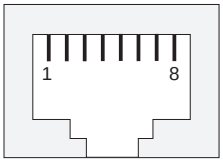
RJ45 (8-pin, MDI) Port Pinouts

Pin	Signal
1	Tx+
2	Tx-
3	Rx+
6	Rx-

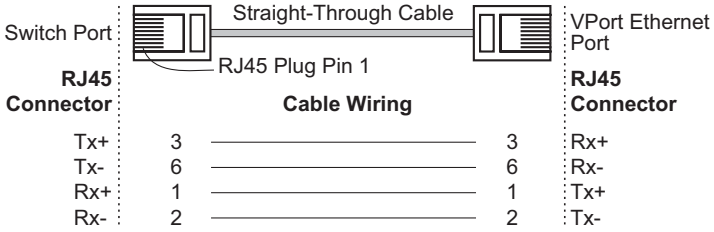


RJ45 (8-pin, MDI-X) Port Pinouts

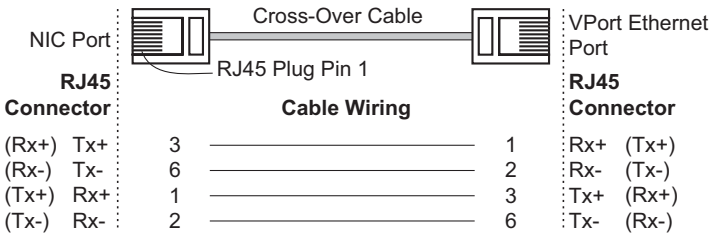
Pin	Signal
1	Rx+
2	Rx-
3	Tx+
6	Tx-



RJ45 (8-pin) to RJ45 (8-pin) Straight-Through Cable Wiring



RJ45 (8-pin) to RJ45 (8-pin) Cross-Over Cable Wiring



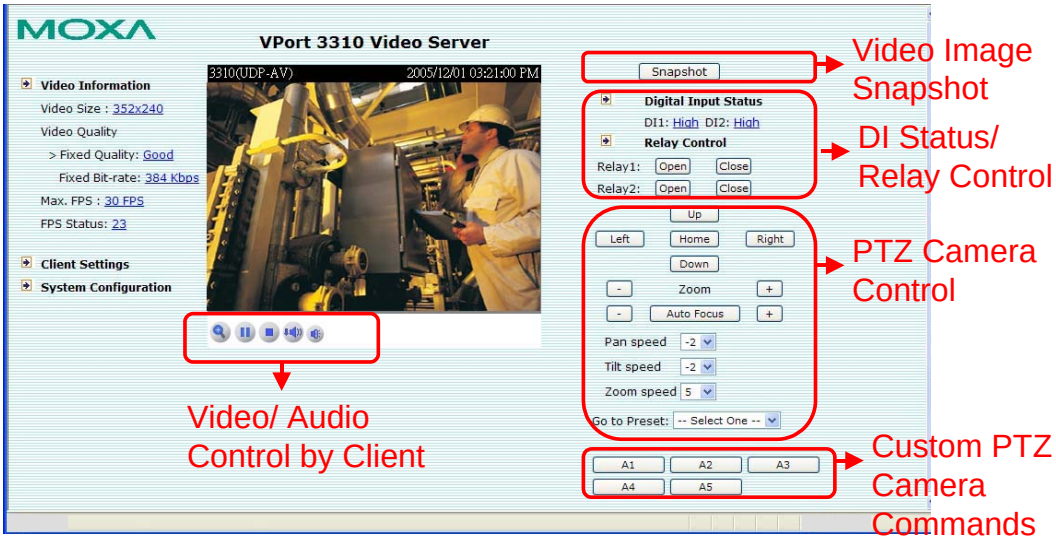
3

Accessing VPort 3310's Web-based Manager

This chapter includes information about how to access VPort 3310 Video Server for the first time. The following topics are covered:

- **Functions Featured on VPort's Homepage**
  - Logo and Host Name
  - Camera Image View
  - Video Information
  - Client Settings
  - System Configuration
  - Video/Audio Control by Clients
  - Video Image Snapshots
  - DI Status/Relay Control
  - Motorized (PTZ) Camera Control
  - Custom PTZ Camera Commands

Functions Featured on VPort's Homepage



Logo and Host Name

The default logo is Moxa's logo, and the host name is VPort 3310 Video Server. For customized usage, the administrator can change the host name of the homepage. The change should be made on the **System Configuration/ System/ General** page.

Camera Image View

The assigned image description and system date/time will be displayed in the caption above the image window. You may disable the caption or change the location of the image information from the **System Configuration/Video/Image Setting**. Note that if VPort's motion detection function is active, some windows in the video picture might be framed in red.

Video Information

Users can easily monitor the current video performance by looking at the **Video Information** shown on the left side of the homepage. The following properties are shown: Video Size, Video Quality, Max. FPS (frames per second), and (current) FPS Status.

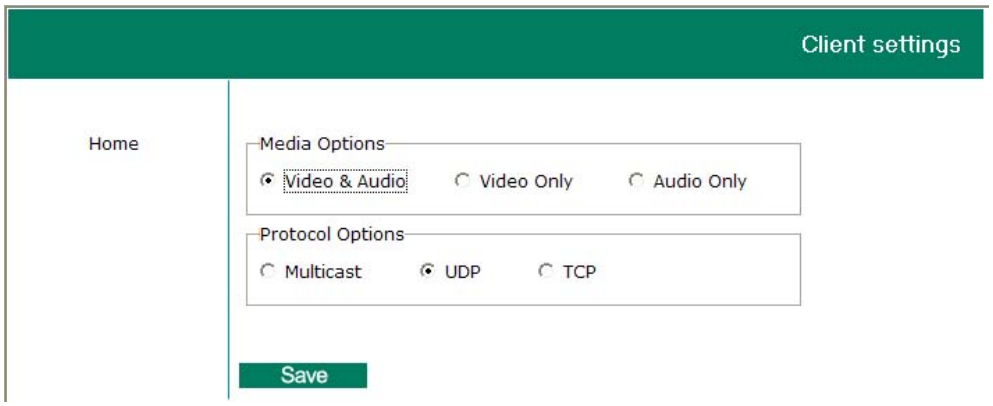
Client Settings

Users can configure the following functions in **Client Settings**.

1. **Media Options**: Enable or disable the video or audio.
2. **Protocol Options**: Choose one of three protocols to optimize your usage—UDP, TCP, or Multicast.
   - **UDP** protocol can be used to produce audio and video streams that are more real-time. However, some packets may be lost due to network burst traffic, and images may become blurred.
   - **TCP** protocol can be used to prevent packet loss, which results in a more accurate video display. The downside of using TCP is that the real-time effect is worse than with UDP protocol.

- **Multicast** protocol can be used to send a single video stream to multiple clients. In this case, a lot of bandwidth can be saved since only 1 video stream is transmitted over the network. However, note that your video server must be set up to use muticast streams, and the network gateway (e.g., a switch) must support a multicast protocol (e.g., IGMP snooping), or the multicast video transmission will not be successful.

Once the Video Server is connected successfully, **Protocol Options** will indicate the selected protocol. The selected protocol will be recorded on the user's PC, and will be used for the next connection.

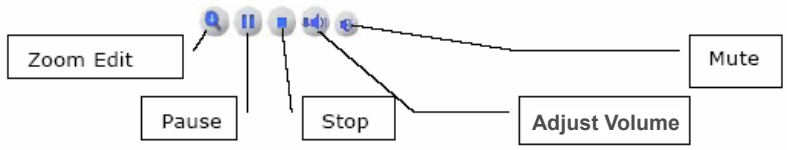


System Configuration

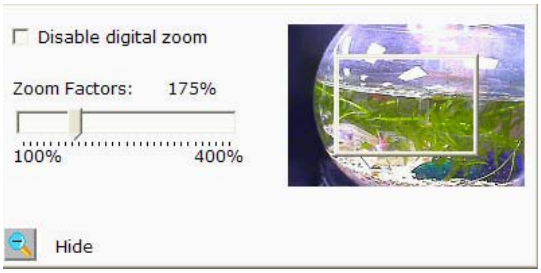
A button or text link on the left side of the system configuration window only appears on the administrator's main page. For detailed system configuration instructions, refer to Chapter 4, **System Configuration**.

Video/Audio Control by Clients

Client users can use the 5 buttons located below the video image to control the audio and video properties.

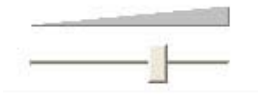


- **Zoom Edit:** Click the **Zoom** button to open the zoom tool in a pop-up window.



- **Pause:** Click the **Pause** button to pause the video. Click the Pause button again to replay the video.
- **Stop:** Click the **Stop** button to close the video screen.

- **Adjust Volume:** Click the **Adjust Volume** button to open the pop-up audio volume-tuning window. Simply move the bar to change the volume.



- **Mute:** Click the **Mute** button to disable the audio. Click the Mute button again to restore the audio.

Video Image Snapshots

Users can take snapshot images for storing, printing, or editing by clicking the **Snapshot** button. To save the image, click the right mouse button and select the **Save** option.

DI Status/Relay Control

VPort 3310 Video Server has 2 DIs and 2 relay outputs for external devices, such as sensors and alarms. The Administrator and other users can check the digital input status. Administrators and permitted users can click on **Open** to short the **Common** and **Normal Open** digital output pins, or click on **Close** to short the **Common** and **Normal Close** digital output pins.

Motorized (PTZ) Camera Control

If a serial device, such as a motorized camera, is attached to the COM port, the control panel will appear on the main page for user's who have permission to operate the camera. Buttons that are active will change color when the cursor is passed over the button. Users can control the pan, tilt, zoom, and focus functions of motorized cameras. The home button is used to return the camera to the center position if the camera supports this command. In addition to near and far control for focus, an AUTO button is provided for setting auto focus mode. To move the motorized camera more precisely, the speed control for pan and tilt allows users to fine tune the aiming of the camera. Users can also click directly on any point in the image to force the motorized camera to focus on that point, or select a preset location from the drop-down menu. Administrators are able to add or modify the list of preset locations. Details are described in the relevant section in Chapter 4, **System Configuration**.

NOTE For some PTZ cameras, users can click on any position on the image to point the camera to that position. We currently support this functionality on Sony EVID30, Cannon VCC4, and Pelco-D PTZ cameras.

Custom PTZ Camera Commands

In addition to the default pan, tilt, zoom, and focus controls, an additional five buttons are available for custom commands to control the attached motorized (PTZ) cameras. Custom commands are set up by administrators, and are used for functions such as activating or deactivating the dome wiper. Refer to the attached motorized device's User's Manual to see which functions can be controlled with these additional buttons.

4

System Configuration

After installing the hardware, the next step is to configure VPort 3310's settings. You may use one of two configuration methods: Web-based manager or FTP.

This chapter includes the following sections:

- **System Configuration via Web-based Manager**
  - VPort Video Server Information
  - System
  - Network
  - Video
  - Audio
  - Alarm
- **System Configuration via FTP**
  - Parameters Available in Config.ini

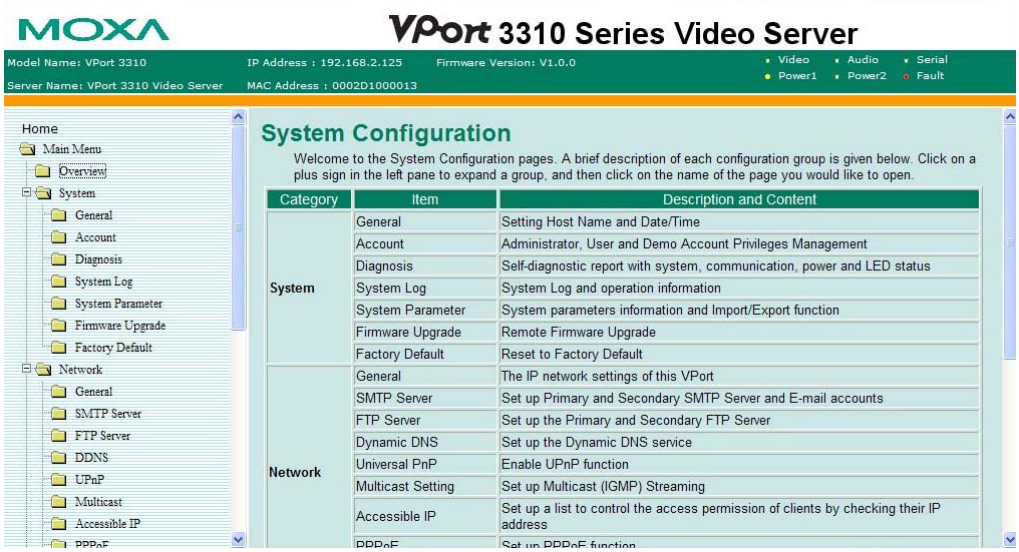
System Configuration via Web-based Manager

System configuration can be done remotely with Internet Explorer via the Web Server. Alternatively, administrators may type the system configuration URL, **http://<IP address of Video Server>/setup/config.html**, to enter the configuration page directly. Administrators who wish to set up certain options by using the URL should refer to the relevant section in Chapter 6, **URL Commands**, for advanced functions.

Five categories of configuration are involved in configuring the system: **System**, **Network**, **Video**, **Audio**, and **Alarm**. A description of each configuration item is shown in the table below:

Category	Item		Description and Contents
System	General		Set Host Name and Date/Time
	Accounts		Administrator, User, and Demo Account Privileges Management
	Diagnosis		Self-diagnostic report with system, communication, power, and LED status
	System Log		System Log and operation information
	System Parameter		System parameters information and Import/Export functions
	Firmware Upgrade		Remote Firmware Upgrade
	Factory Default		Reset to Factory Default
Network	General		The IP network settings of this VPort
	SMTP Server		Set up Primary and Secondary SMTP Server and e-mail accounts
	FTP Server		Set up the Primary and Secondary FTP Server
	Dynamic DNS		Set up the Dynamic DNS service
	Universal PnP		Enable UPnP function
	Multicast		Set up Multicast (IGMP) Streaming
	IP Filtering		Set up a list to control the access permission of clients by checking their IP address
	PPPoE		Set up the PPPoE function
	SNMP		SNMP Settings
Video	Image Setting		Configure the attributes of the video image
	Camera Modulation		Select the camera's modulation (NTSC, PAL or AUTO)
	Video Performance		Set up the Size (Resolution), FPS, and Video Quality
	Camera Control		Set up the Camera's PTZ Control
Audio	Quality		Set up the bit rate for audio quality and audio source
Alarm	System Alarm		Configure Power Failure, Video Loss, and Network Connection Broken alarms
	Event Alarm	Basic	General settings of event alarm
		Schedule	Set up the Alarm schedule
		Video Motion Detection	Configure the Video Motion Detection Alarm
		Digital Input	Configure the Digital Input Alarm
		Sequential Snapshot	Set up the Sequential Snapshot operation

You can also find this table on the **System Configuration → Overview** webpage.



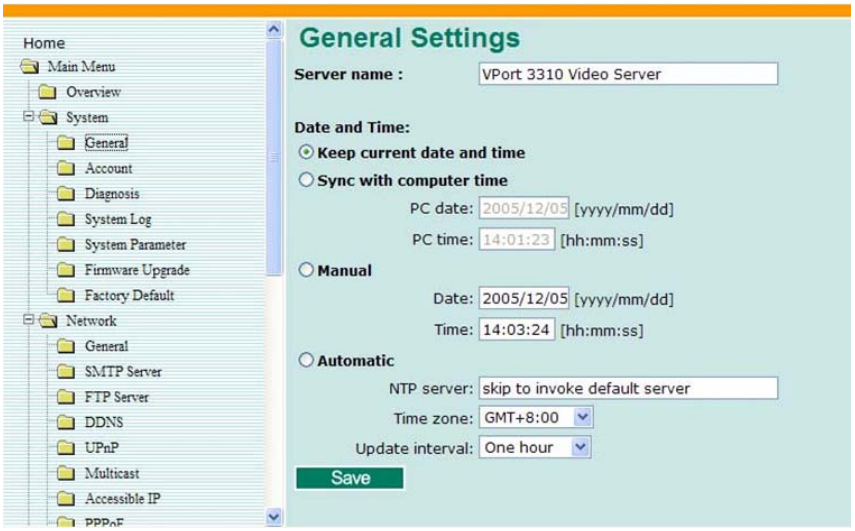
VPort Video Server Information

Information is displayed at the top of each system configuration webpage. In addition to the MOXA logo and product line name, you can also see the model name, sever name, IP address, MAC address, firmware version, and the LED status of this VPort 3310. This information can help the administrator get a clearer picture of how the VPort operates.

System

General Settings

On the **General Settings** page, administrators can set up the video **Server name** and the **Date and Time**, which appear in the image's caption.



Server name

Setting	Description	Default
Max. 40 characters	Use a different server name for each server to help identify the different servers. The name appears on the web homepage.	VPort 3310 Video Server

Date and Time

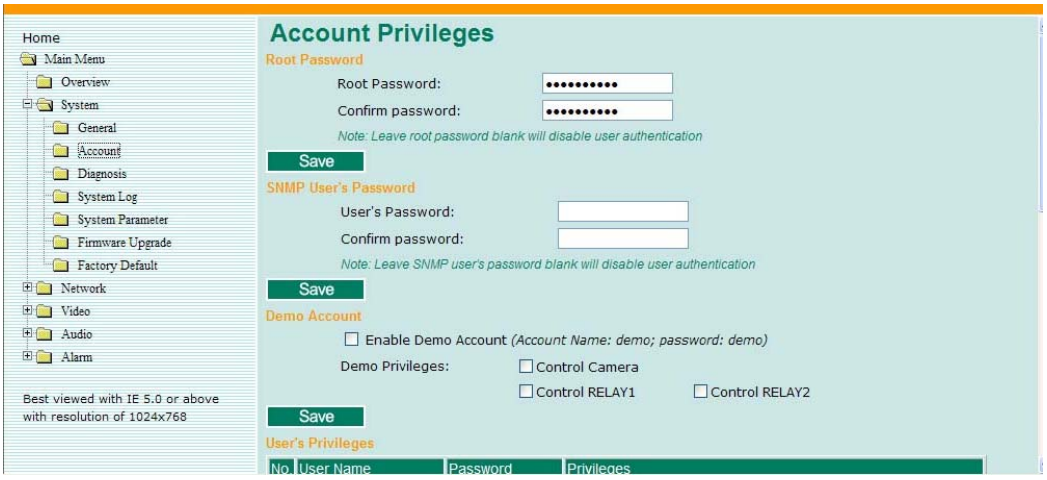
Setting	Description	Default
Keep current date and time	Use the current date and time as the VPort's time setting.	VPort 3310 Video Server
Sync with computer time	Synchronize VPort's data and time setting with the local computer time.	
Manual	Manually change VPort's date and time setting.	
Automatic	Use the NTP server for changing VPort's date and time setting in a given period.	

NOTE Select the **Automatic** option to force the VPort to synchronize automatically with timeservers over the Internet every month. However, synchronization may fail if the assigned **NTP server** cannot be reached, or the VPort is connected to a local network. Leaving the **NTP server** blank will force the VPort to connect to default timeservers. Enter either the Domain name or IP address format of the timeserver if the DNS server is available.

Don't forget to set the **Time zone** for local settings. Refer to Appendix G for your region's time zone.

Account Privileges

Different account privileges are available for different purposes.



Root password

Setting	Description	Default
Root Password (max. 14 characters)	Administrator can type the new password in this box.	Default root password is "root"
Confirm Password (max. 14 characters)	If a new password is typed in the **Root Password** box, you will need to retype the password in the **Confirm Password** box before updating the new password.	

NOTE The default account name for administrator is **root**; the administrator account name cannot be changed.

SNMP User's Password

SNMP user accounts are used to authenticate users by SNMP (except for administrator). The default username is **User**; this username cannot be changed.

Setting	Description	Default
User's Password (max. 14 characters)	Administrator can type new password in this box.	None
Confirm Password (max. 14 characters)	If a new password is typed in the **User's Password** box, you must retype the password in the **Confirm Password** box before updating the new password.	

Demo Account

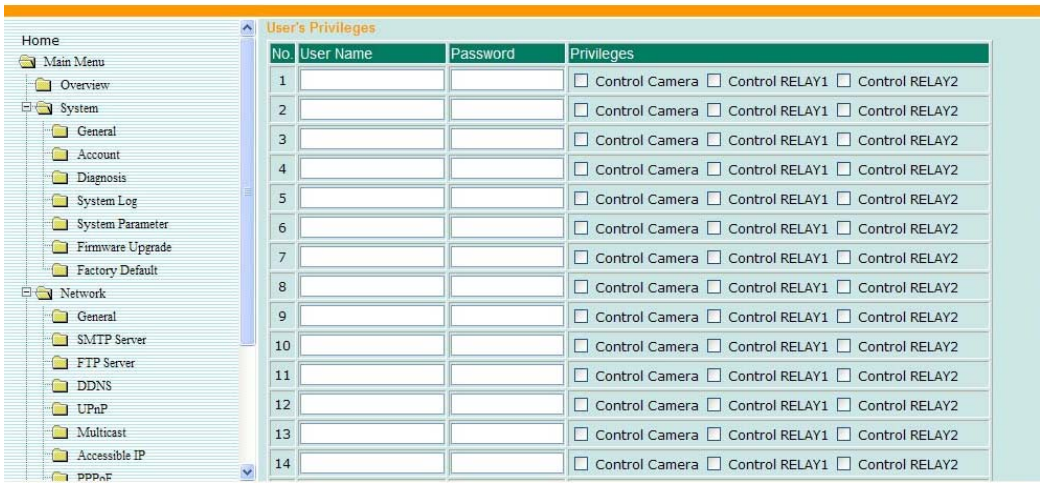
Administrators can check the function box of **Enable Demo Account** to enable the demo account for users not in the user account. The account is **demo** and the password is **demo**. The following demo account privileges can be configured.

Setting	Description	Default
Control Camera	Check this function box to enable PTZ camera control.	None
Control Relay1	Check this function to enable relay1 control.	
Control Relay2	Check this function box to enable relay2 control.	

User's Privileges

VPort products provide 20 user accounts for accessing VPort. Administrators can set up each user's privileges in this section. Each user can be given independent access right to the external I/O and camera control.

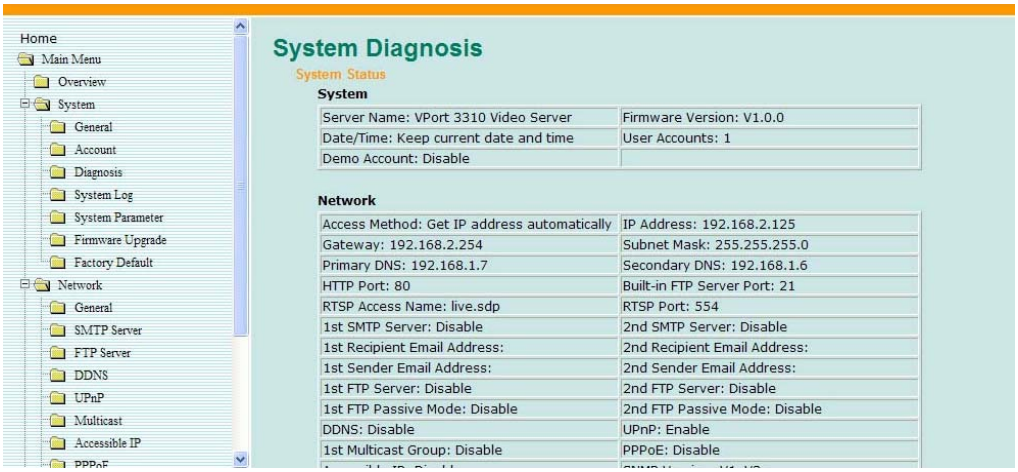
Setting	Description	Default
User Name	Type a specific user name for each user's authentication.	None
Password	Type a specific password for each user's authentication.	
Privilege	Check the function boxes to determine each user's privileges in **Control Camera**, **Control Relay1**, and **Control Relay2**.	



NOTE The FPS of the video stream will be reduced as more and more users access VPort. For this reason, only 10 user's accounts can access VPort 3310 at the same time. Enforcing this kind of restriction helps guarantee the performance of the video stream.

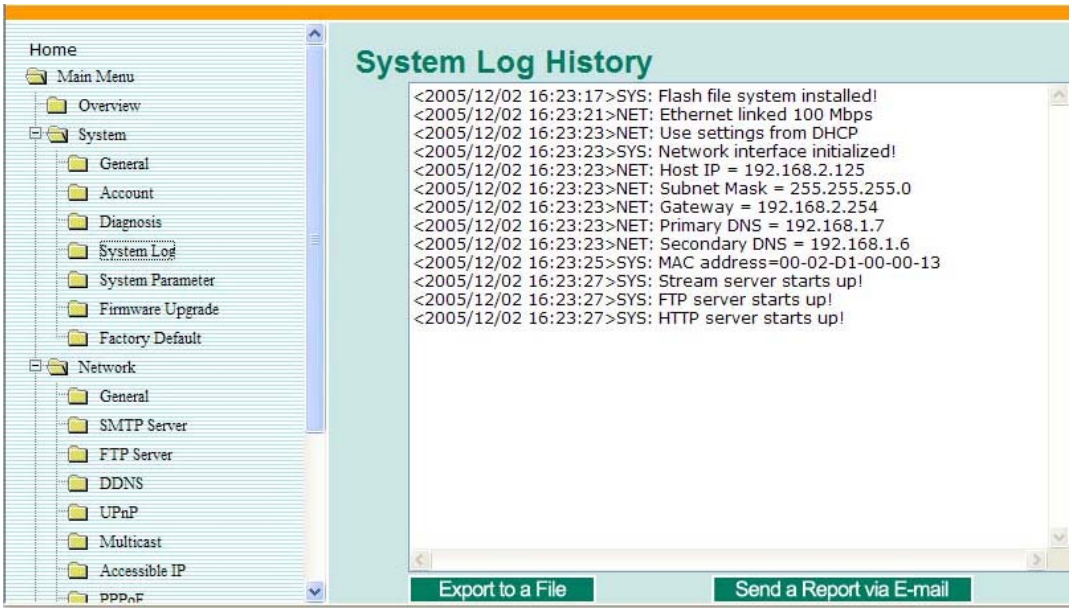
System Diagnosis

VPort products have a self-diagnosis function to let the administrator get a quick view of the system and connection status. Administrators can save this diagnosis information in a file (diagnosis.log) by clicking **Export to a File** button, or send the file via email by clicking **Send a Report via Email** button.



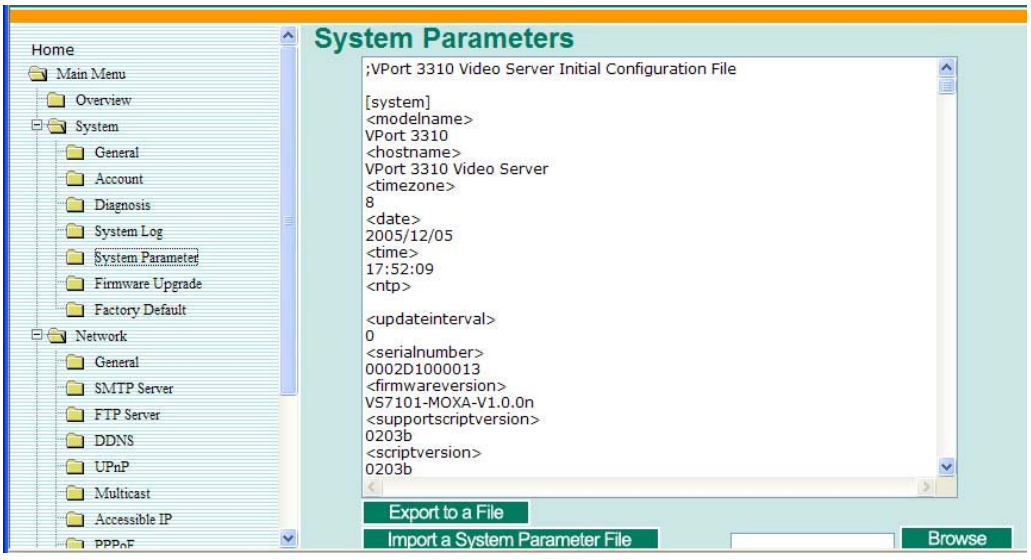
System Log History

The system log contains useful information, including current system configuration and activity history with timestamp for tracking. Administrators can save this information in a file (system.log) by clicking **Export to a File** button, or send the file via email by clicking **Send a Report via Email** button.



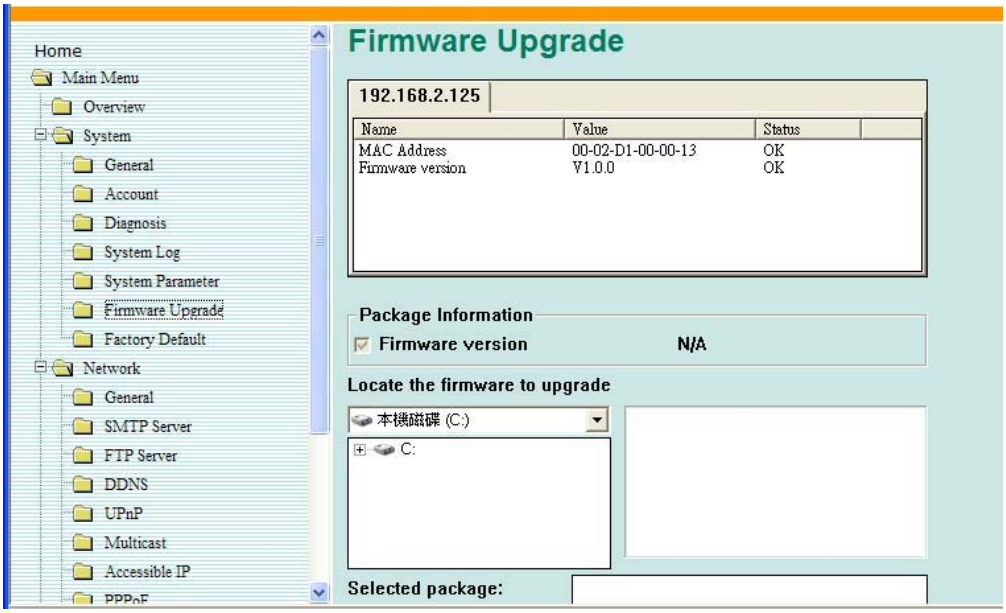
System Parameters

The **System Parameters** page allows you to view all system parameters, which are listed by category. The content is the same as VPort's CONFIG.INI file. Administrators can also can save this information in a file (config.ini) by clicking the **Export to a File** button, or import a file by clicking the **Import a System Parameter File** button to update all the system configurations quickly.



NOTE The system parameter import/export functions provide the administrator with a quick method of updating system configurations, especially for a system that includes several VPort video servers. The Administrator can export this CONFIG.ini file, change settings using a text edit tool, and then import the CONFIG.ini file to the VPort video servers. System configurations will be changed immediately after the VPort is rebooted.

Firmware Upgrade



Take the following steps to upgrade the firmware:

Step 1: Select the firmware from the **Locate the firmware to upgrade** drop-down list.

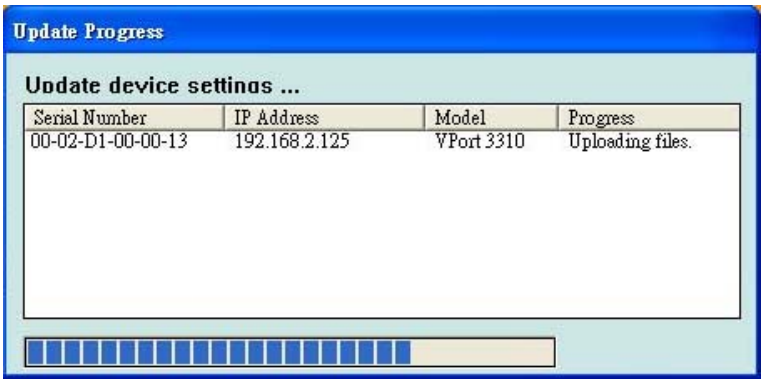
NOTE For VPort 3310, the firmware file extension should be **pkg**.

Step 2: The selected firmware version is showed on the **Package Information.**

Step 3: Make sure the firmware version you choose is correct or newer than the version shown at the top of the page.

Step 4: If the firmware file is correct, click on the **Upgrade**. If the firmware version is out of date, or equal to the current firmware version, a warning message will pop-up to ask if you want to process the upgrade.

Step 5: At this point, an **Update Progress** pop-up window will show you the progress of the firmware upgrade. When the process is finished, a **Done** button will appear in the right corner of the window. Click on the **Done** button to complete the entire upgrade process.



Reset to Factory Default

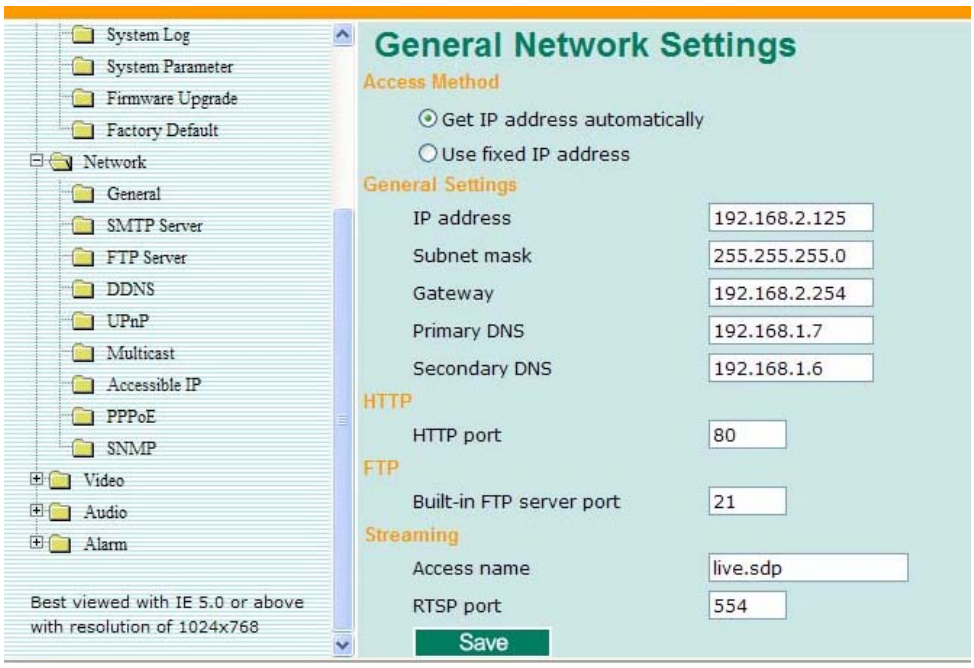
Reset to the factory default by clicking on the **OK** button (as shown in the following figure).

NOTE All parameters will be reset to the factory defaults when you use the **Factory Default** function. For this reason, remember to export the CONFIG.ini file before using the Factory Defaul function if you want to keep the customized configuration file.

Network

General Network Settings

The **General Network Settings** page includes some basic but important network configurations that enable the VPort to be connected to a TCP/IP network.



Access Method

VPort products support the DHCP protocol, which means that VPort can get its IP address from a DHCP server automatically when it is connected into the TCP/IP network. The Administrator should determine if it is more appropriate to use DHCP, or assign a fixed IP.

Setting	Description	Default
Get IP address automatically	VPort gets the IP address automatically from the DHCP server.	Get IP address automatically
Use fixed IP address	Use the IP address assigned by the administrator.	

NOTE We strongly recommend that the administrator assign a fixed IP address to the VPort, since all of the functions and applications provided by VPort are active when VPort is connected to the network. Use DHCP to determine if the VPort's IP address may change when then network environment changes, or the IP address is occupied by other clients.

General Settings

Setting	Description	Default
IP address	Variable IP assigned automatically by the DHCP server, or fixed IP assigned by the Administrator.	192.168.0.99
Subnet mask	Variable subnet mask assigned automatically by the DHCP server, or a fixed subnet mask assigned by the Administrator.	255.255.255.0
Gateway	Assigned automatically by the DHCP server, or assigned by the Administrator.	blank
Primary DNS	Enter the IP address of the DNS Server used by your network. After entering the DNS Server's IP address, you can input VPort's url (e.g.,www.VPort. company.com) in your browser's address field, instead of entering the IP address.	Automatically get from DHCP server, or blank in non-DHCP environment
Secondary DNS	Enter the IP address of the DNS Server used by your network. VPort will try to locate the secondary DNS Server if the primary DNS Server fails to connect.	Automatically get from DHCP server, or blank in non-DHCP environment

HTTP

Setting	Description	Default
HTTP Port (80, or 1024 to 65535)	HTTP port enables connecting VPort to the web.	80

FTP

Setting	Description	Default
Built-in FTP server port (21, or 1024 to 65535)	Local FTP server port enables connecting VPort to FTP.	21

Streaming

VPort 3310 supports standard RTSP (Real Time Streaming Protocol) streaming, which means that all devices and software that support RTSP can directly acquire and view the video images sent from VPort 3310 without any proprietary codec or SDK installations, for the convenience of network system integration. The default access name is live.sdp, which means that you can access the media through the following URL: rtsp://<IP address>/live.sdp in the software that supports RTSP.

Setting	Description	Default
Access Name (max. 20 characters)	A URL to identify VPort's RTSP video/audio stream.	live.sdp
RTSP Port	An RTSP port is similar to an HTTP port, which can enable the connection of video/audio stream via RTSP.	554

We use Apple QuickTime media player to illustrate RTSP streaming applications:

Step 1: Open Apple QuickTime Player and select **File → Open URL in New Player**.

Step 2: When the following pop-up window appears, type the URL in the input box. E.g., type **rtsp://<VPort 3310's IP address>/live.sdp**, and then click on **OK** to connect to VPort 3310.

Step 3: Wait a few seconds for QuickTime Player to establish the connection.

Step 4: After the connection has been established, VPort 3310's video will appear in the QuickTime Player display window.

NOTE The video performance of VPort 3310 in other media players may not always be the same. For example, you will notice a greater delay when viewing VPort 3310's video from QuickTime player compared to viewing it directly from VPort 3310's built-in web server. In addition, viewing VPort 3310's video from Quicktime player through a router or Internet gateway could result in a broken connection.

NOTE For the time being, VPort 3310's RTSP video/audio stream can be identified and viewed by Apple QuickTime Ver. 6.5 and above, and RealPlayer Ver.10.5 and above. System integrators can use these 2 media players to view VPort 3310's video directly, without needing to use VPort's SDK to create customized software.

SMTP Server and Email Account Settings

VPort Video Servers not only play the role of server, but can also connect to outside servers to send alarm messages or snapshots. If the administrator has set up some applications in either system information or alarm, the VPort will send out messages or snapshots once these conditions occur.

1st SMTP Server and Sender Email

Setting	Description	Default
1st SMTP (mail) server	SMTP Server's IP address or URL address.	None
1st SMTP account name	For security reasons, most SMTP servers require the account name and password to be authenticated.	None
1st SMTP password		None
1st Sender's email address	For security reasons, SMTP servers must see the exact sender email address.	None

NOTE Note that if the **Sender's email address** is not set, a warning message will pop up and the e-mail system will not be allowed to operate.

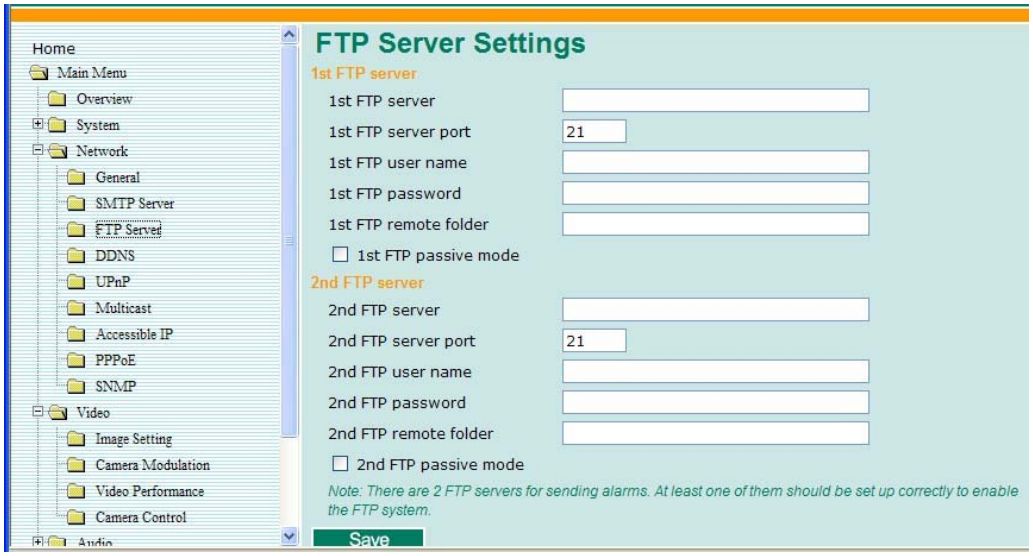
*NOTE: The **2nd SMTP Server and Sender Email** are backups that are used if the 1st SMTP Server and Sender Email fail when connecting or sending email.*

Two recipient email accounts are available for receiving emails sent by VPort. For redundancy, both addresses receive the sending messages and alarm snapshots simultaneously.

Setting	Description	Default
1st Recipient's Email Address	Email address of the 1st recipient.	None
2nd Recipient's Email Address	Email address of the 2nd recipient.	None

FTP Server Settings

FTP is the other method available for VPort Video Servers to send alarm messages and snapshots.



1st FTP Server

Setting	Description	Default
1st FTP server	FTP server's IP address or URL address.	None
1st FTP server port	FTP server's authentication.	None
1st FTP user name		None
1st FTP remote folder	FTP file storage folder on the remote FTP server.	None
1st FTP passive mode	Passive transfer solution for FTP transmission through a firewall.	Disabled

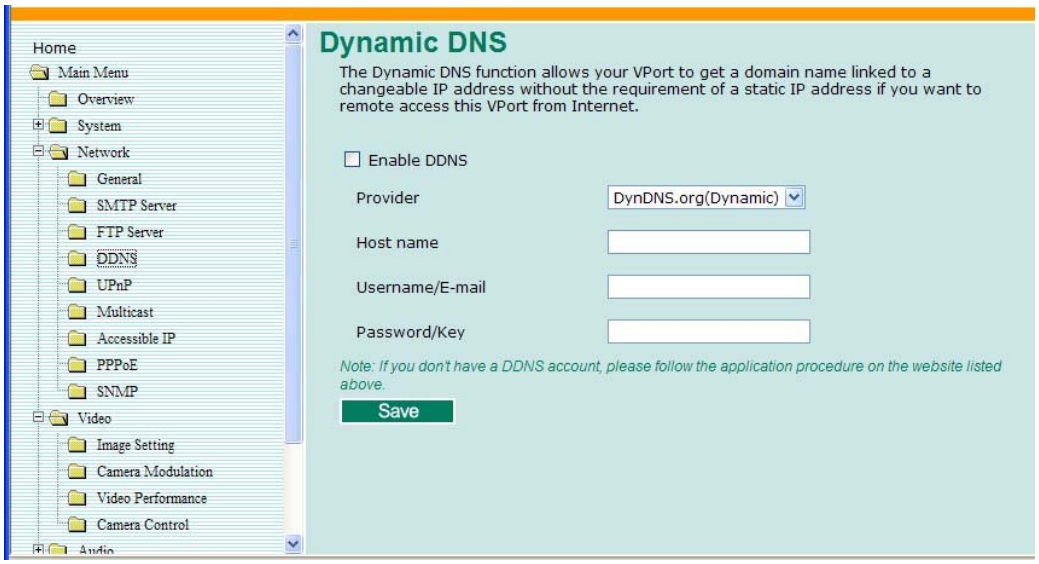
*NOTE: The **2nd FTP Server** is a backup in case the 1st FTP Server fails to connect or has trouble sending files.*

NOTE Whenever the system reboots, a system log will be sent by email or FTP to show the login status of the VPort. The system log will be sent to the Sender email address if the SMTP server settings are correct. To send the system log via FTP, the SMTP server should be erased since the E-mail system is used by default to transmit the system log.

NOTE In either e-mail or FTP, the 1st server information should be entered first. If the 1st server is not set, the related FTP or email will be cancelled. Note that it may take time to connect to the 2nd server after the first server fails, and it may affect some applications when adverse conditions occur too often.

Dynamic DNS

DDNS (Dynamic Domain Name System) is a combination of DHCP, DNS, and client registration. DDNS allows administrators to alias VPort's dynamic IP address to a static hostname in any of the domains provided by the DDNS service providers listed on VPort's Network/DDNS configuration page. DDNS makes it easier to access VPort from various locations on the Internet.



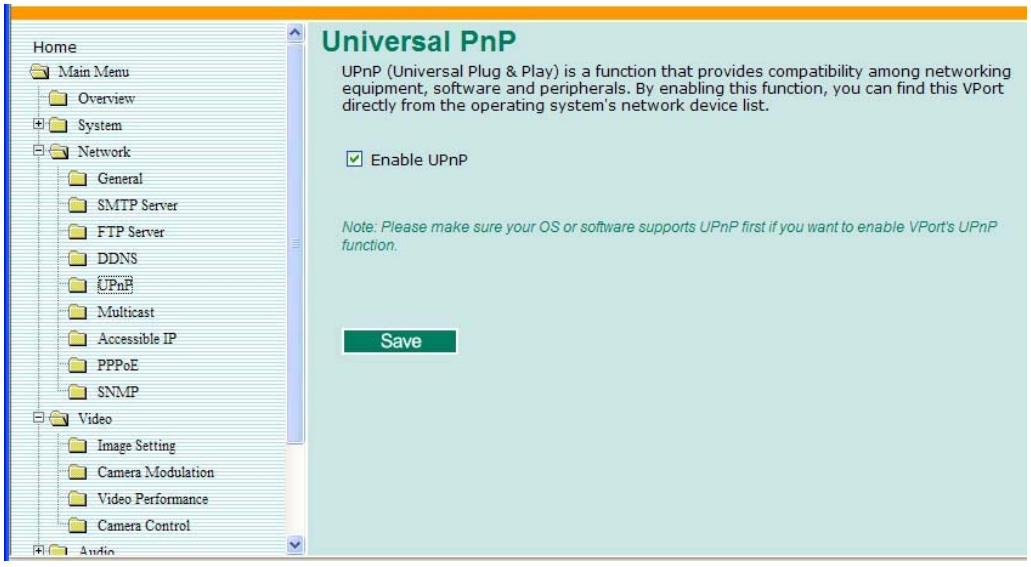
Setting	Description	Default
Enable DDNS	Enable or disable DDNS function.	Disable
Provider	Select the DDNS service providers, including DynDNS.org (Dynamic), DynDNS.org (Custom), TZO.com, and dhs.org.	None
Host Name	The Host Name you use to link to VPort.	None
Username/ E-mail	The Username/E-mail and Password/Key are used to enable the service from the DDNS service provider (based on the rules of DDNS websites).	None
Password/ Key		None

NOTE Dynamic DNS is a very useful tool for accessing VPort via the Internet, especially for xDSL connections with a non-fixed IP address (DHCP). Administrator and users can avoid the trouble of connecting with VPort when the IP address of VPort is not fixed by using the unique host name in the URL to establish a connection with VPort.

NOTE Different DDNS service providers have different application rules. Some applications are free of charge, but most require an application fee.

Universal PnP

UPnP (Universal Plug & Play) is a networking architecture that provides compatibility among networking equipment, software, and peripherals of the 400+ vendors that are part of the Universal Plug and Play Forum. This means that they are listed in the network devices table for the operating system (such as Windows XP) supported by this function. Users can link to VPort directly by clicking on the VPort listed in the network devices table.



Setting	Description	Default
Enable UPnP	Enable or disable UPnP function.	Enable

Multicast

VPort 3310 supports the advanced Multicast network protocol-IGMP, which can greatly improve the efficiency of network traffic. In this section, we explain multicasts, multicast filtering, and how multicast can be implemented on your VPort.

What is Multicast?

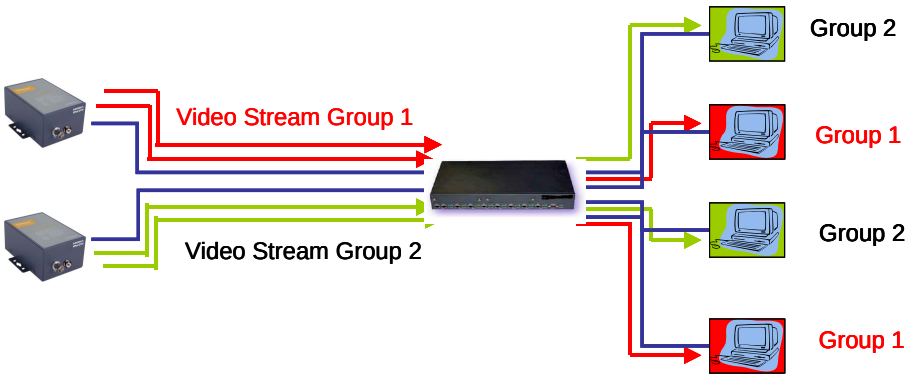
A multicast is a packet that is intended for "one-to-many" and "many-to-many" communication. Users explicitly request to participate in the communication by joining an end-station to a specific multicast group. If the network is set up correctly, a multicast can only be sent to an end-station or a subset of end-stations in a LAN, or VLAN, that belong to the relevant multicast group. Multicast group members can be distributed across multiple subnetworks; Therefore, multicast transmissions can occur within a campus LAN or over a WAN. In addition, networks that support IP multicast send only one copy of the desired information across the network. The packets are only replicated if they reach a network node that links to two or more members of the multicast network. Transmitting packets in this way makes more efficient use of network bandwidth. A multicast packet is identified by the presence of a multicast group address in the destination address field of the packet's IP header.

Benefits of Multicast

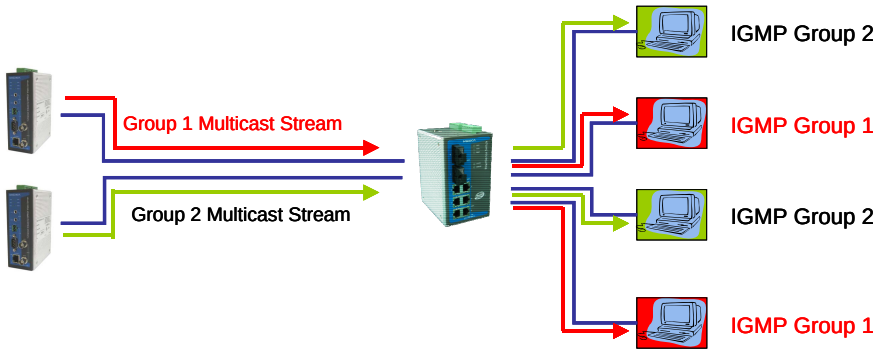
The benefits of using IP multicast are that it:

- Enables the simultaneous delivery of information to many receivers in the most efficient, logical way.
- Reduces the load on the source (for example, a server) because it does not need to produce multiple copies of the same data.
- Makes efficient use of network bandwidth and scales well as the number of participants or collaborators expands.
- Works with other IP protocols and services, such as Quality of Service (QoS).
- There are situations where a multicast approach is more logical and efficient than a unicast approach. A typical use of multicasts is in video-conferencing, in which high volumes of traffic need to be sent to several end-stations simultaneously, but for which broadcasting that traffic to all end-stations would seriously reduce network performance. Besides, several industrial automation protocols, such as Allen-Bradley, EtherNet/IP, Siemens Profibus, and Foundation Fieldbus HSE (High Speed Ethernet), use the multicast approach. These industrial Ethernet protocols use publisher/subscriber communications models by multicasting packets that could flood a network with heavy traffic. IGMP provides the ability to prune multicast traffic so that it travels only to those end destinations that require the traffic, thus reducing the amount of traffic on the Ethernet LAN.

The network WITHOUT Multicast

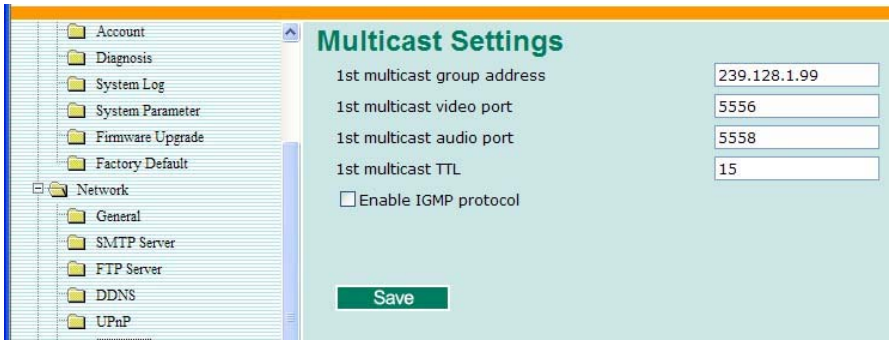


The network WITH Multicast



NOTE VPort 3310 is the source that delivers the multicast video stream. To benefit from the Multicast protocol, the gateway or network switch should support the multicast filtering function (such as IGMP Snooping) so that the multicast stream is delivered correctly and precisely. To learn more about IGMP Snooping, refer to the MOXA EtherDevice™ series Industrial Ethernet Switch user's manual.

Configuring Multicast Settings

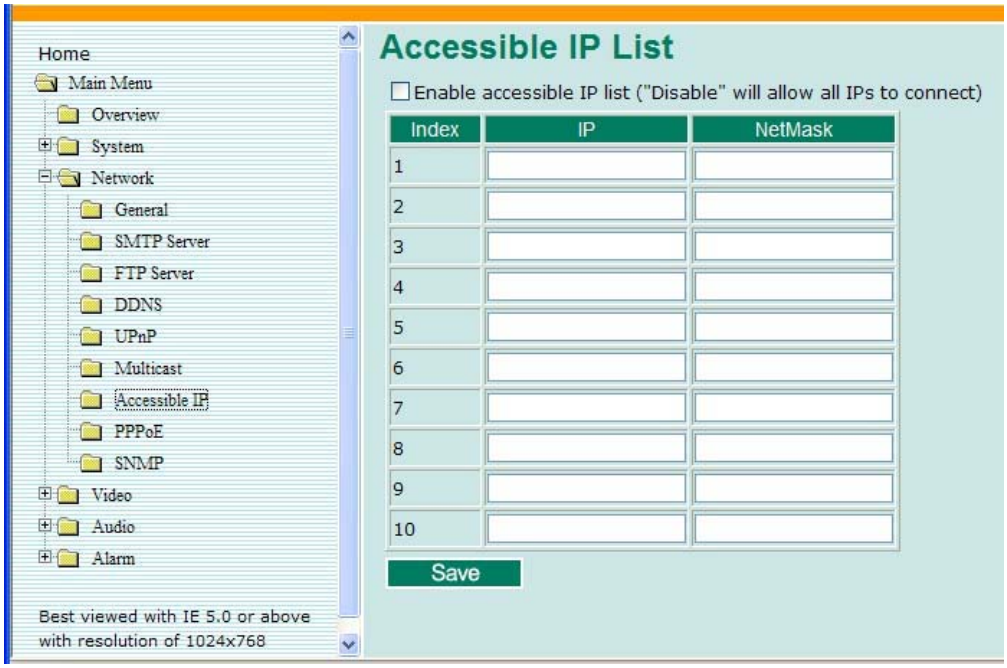


Setting	Description	Default
1st multicast group address	Multicast Group address for sending video stream.	239.128.1.99
1st multicast video port	Video port number.	5556
1st multicast audio port	Audio port number.	5558
1st multicast TTL	Multicast-TTL (Time-to-live) threshold. In the network, there is a certain TTL threshold defined for each network interface or tunnel. A multicast packet's TTL must be larger than the defined TTL for that packet to be forwarded across that link.	15
Enable IGMP protocol	Enable or disable the IGMP Multicast steam of VPort.	Disable

NOTE Whenever you enable the IGMP Multicast stream of VPort, please note the video/audio port number.

Accessible IP List

VPort 3310 uses an IP address-based filtering method to control access to the VPort.



Accessible IP Settings allows you to add or remove "Legal" remote host IP addresses to prevent unauthorized access. Access to VPort is controlled by IP address. That is, if a host's IP address is in the accessible IP table, then the host will be allowed access to the VPort. Administrators can allow one of the following cases by setting this parameter:

- Only one host with a specific IP address can access the VPort.
  Enter "IP address/255.255.255.255" (e.g., 192.168.1.1/255.255.255.255)
- Hosts on a specific subnet can access the VPort.
  Enter "IP address/255.255.255.0" (e.g., "192.168.1.0/255.255.255.0")
- Any host can access the VPort.
  Disable this function.

Refer to the following table for more configuration examples.

Allowable Hosts	Input Formats
Any host	Disable
192.168.1.120	192.168.1.120/255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0/255.255.255.0
192.168.0.1 to 192.168.255.254	192.168.0.0/255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0/255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128/255.255.255.128

PPPoE

Some environments do not have a LAN, and therefore alternative solutions, such as an xDSL connection, are used for setting up the remote network system. VPort 3310 supports the PPPoE (PPP over Ethernet) function, which means that VPort 3310 can dial up to the ISP server by itself to request an IP address.

Video Server WITHOUT PPPoE

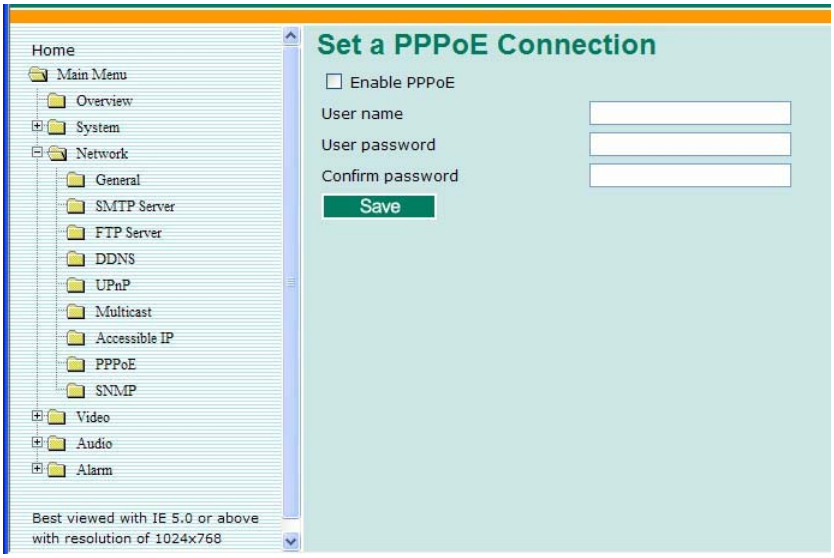
In this case, a router with PPPoE is required for dial up to ISP and the IP address must be fixed to retain the video server's network connection.

Video Server WITH PPPoE

The PPPoE function allows VPort 3310 to dial up to an ISP automatically. In this case, VPort does not need to use a fixed IP address, since an email will be sent to notify the administrator that the current IP address was changed by the ISP server. The PPPoE function is more cost-effective compared to applying for a fixed IP address.

How to establish VPort 3310's PPPoE connection

Step 1: Configure VPort 3310's PPPoE configuration page via a private LAN connection.



Setting	Description	Default
Enable PPPoE	Enable or disable PPPoE function.	Disable
User name	Authentication is given to the ISP to establish the xDSL connection.	None
User password		None
Confirm password		None

Step 2: Configure the SMTP server for setting up **Recipient's Email Address** to send the assigned IP address if this xDSL connection is a dynamic IP address.

Step 3: Power off the VPort 3310 and change the LAN connection to an xDSL connection.

Step 4: Power on the VPort 3310, and wait a few seconds for VPort 3310 to establish the xDSL connection.

Step 5: Check the email of the given recipient's email address to get the IP address assigned by the ISP for this xDSL connection.

NOTE The DDNS function provides a good means of accessing VPort 3310 when using a dynamic IP. DDNS assigns a fixed URL to the VPort 3310, so that the Administrator does not need to go through the trouble of checking if the IP address assigned by ISP has changed. For more information, please refer to the DDNS function description in a previous section.

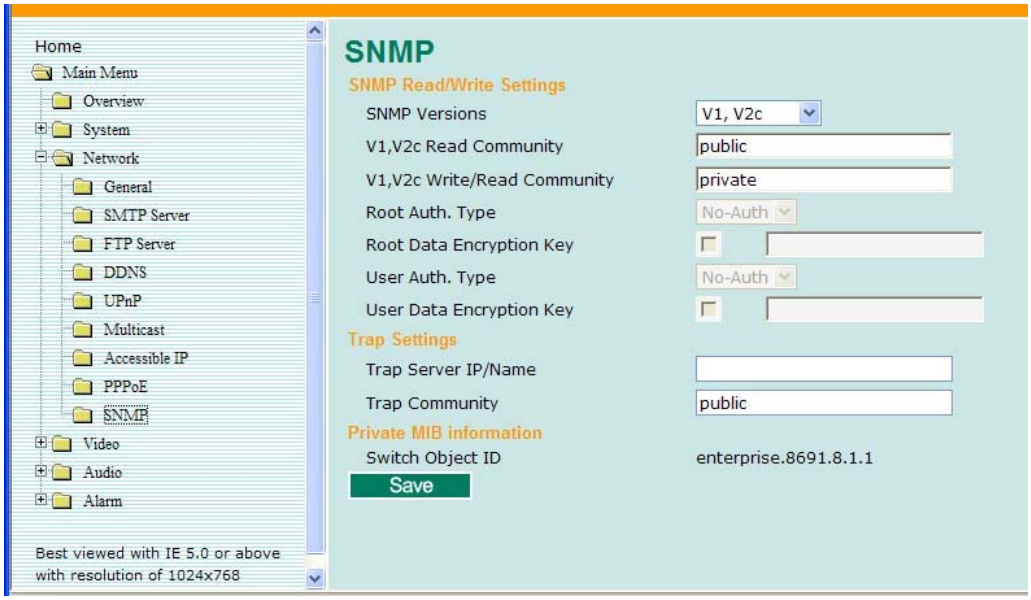
SNMP

VPort supports three SNMP protocols. The available protocols are SNMP V1, SNMP V2c, and SNMP V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions using the community string **public/private** (default value). SNMP V3, which requires you to select an authentication level of MD5 or SHA, is the most secure protocol. You can also enable data encryption to enhance data security. SNMP security modes and security levels supported by VPort are shown in the following table. Select one of these options to communicate between the SNMP agent and manager.

Protocol Version	Security Mode	Authentication Type	Data Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Use a community string match for authentication
	V1, V2c Write/Read Community	Community string	No	Use a community string match for authentication
SNMP V3	No-Auth	No	No	Use account with admin or user to access objects
	MD5 or SHA	MD5 or SHA	No	Provides authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.
	MD5 or SHA	MD5 or SHA	Data encryption key	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key. 8-character passwords and a data encryption key are the minimum requirements for authentication and encryption.

Configure SNMP

The following figures indicate which SNMP parameters can be configured. A more detailed explanation of each parameter is given below the figure.



SNMP Read/Wirte Settings

SNMP Versions

Setting	Description	Default
V1, V2c, V3	Select SNMP Versions V1, V2c, V3 protocol to manage the switch.	V1, V2c
V1, V2c	Select SNMP Versions V1, V2c protocol to manage the switch.	
V3 only	Select SNMP Versions V3 protocol only to manage the switch.	

V1, V2c Read Community

Setting	Description	Default
V1, V2c Read Community	Use a community string match for authentication. The SNMP agent uses the community string **public** to access all objects with read-only permission.	Public (max. 30 characters)

V1, V2c Read/Write Community

Setting	Description	Default
V1, V2c Read/Write Community	Use a community string match for authentication. The SNMP agent uses the community string **public** to access all objects with read-only permission.	Public (max. 30 characters)

For SNMP V3, there are two levels of privilege for different accounts to access the VPort. Admin privilege allows access and authorization to read and write the MIB file. User privilege only allows reading MIB file, but does not authorize writing to the file.

Root Auth. Type (for SNMP V1, V2c, V3, and V3 only)

Setting	Description	Default
No-Auth	Use admin. account to access objects. No authentication.	No
MD5-Auth	Provides authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	No
SHA-Auth	Provides authentication based on the MAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	No

Root Data Encryption Key (for SNMP V1, V2c, V3, and V3 only)

Setting	Description	Default
Enable	8-character data encryption key is the minimum requirement for data encryption. The maximum is a 30-character encryption key.	No
Disable	No data encryption.	No

User Auth. Type (For SNMP V1, V2c, V3, and V3 only)

Setting	Description	Default
No-Auth	Use the admin account or user to access objects. No authentication.	No
MD5-Auth	Provides authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	No
SHA-Auth	Provides authentication based on the HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	No

User Data Encryption Key (For SNMP V1, V2c, V3, and V3 only)

Setting	Description	Default
Enable	8-character data encryption key is the minimum requirement for data encryption. The maximum is a 30-character encryption key	No
Disable	No data encryption	No

Trap Settings

Setting	Description	Default
Trap Server IP/Name	Enter the IP address or name of the Trap Server used by your network.	No
Trap Community	Use a community string match for authentication; The maximum is 30 characters.	No

Private MIB information

The private SNMP Object ID of the VPort is the enterprise value: 8691.8.1.1. This number cannot be changed.

Video

Image Settings

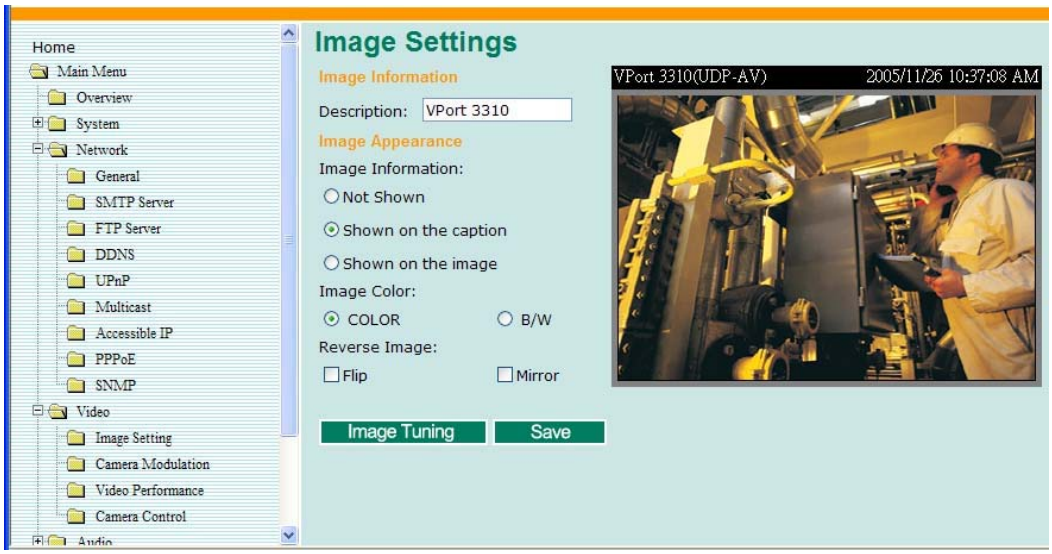


Image Information

Setting	Description	Default
Description (max. of 14 characters)	The customized description shown on the caption or image to identify this video camera.	None

Image Appearance

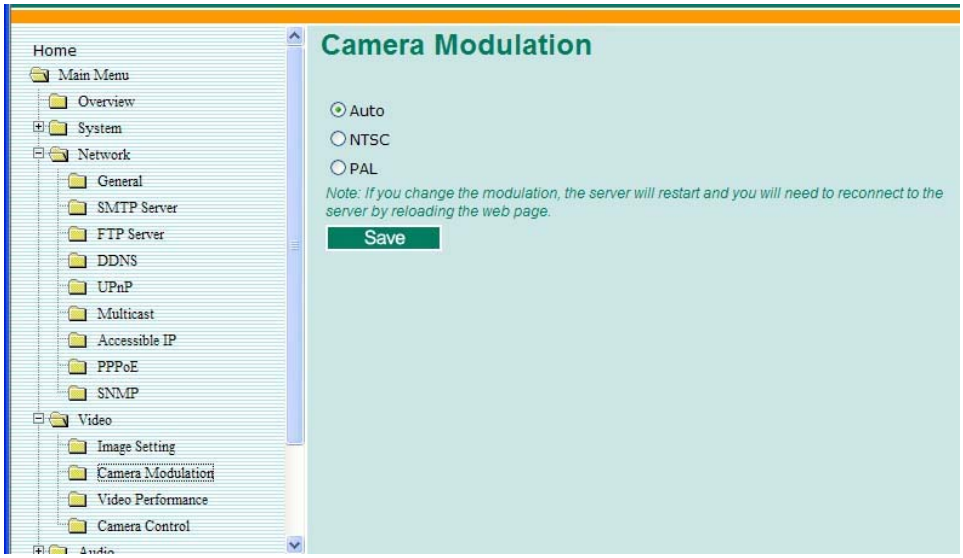
Setting	Description	Default
Image Information	To determine what style of image information is being shown. Includes **Not Shown, Shown on the Caption**, and **Shown on the Image**.	Shown on the caption
Image Color	Determines if the camera image is **COLOR** or **B/W** (black and white).	Color
Reverse Image	The Administrator can change the direction of the image to be shown using **Flip** or **Mirror**.	None

Image Tuning

An Image Tuning button is available for the administrator to fine tune image attributes. After clicking this button, a configuration window will pop up. You may configure **Brightness**, **Contrast**, **Saturation**, and **Hue**.

Camera Modulation

VPort supports both NTSC and PAL camera modulations. The Administrator can use automatic sensing by selecting **Auto**, or manually select **NTSC** or **PAL**.



NOTE Changing the modulation requires resetting the server to detect the camera. Please ensure that your configurations are saved before resetting the server.

Video Performance

Resolution

Setting	Description	Default
Select the image size	4 image resolutions (size) are provided. The administrator can choose each option with NTSC or PAL modulation.	352 × 240 in NTSC or 352 × 288 in PAL

NTSC	PAL
176 × 120	176 × 144
352 × 240	352 × 288
640 × 480	640 × 480
704 × 480	704 × 576

Frame Rate (Frame per second)

Setting	Description	Default
Maximum frame rate	Each resolution has a maximum frame rate limit due to the system performance.	30 for NTSC 25 for PAL
Key frame interval	The Administrator can set up the key frame interval to determine the video quality.	120

NTSC	Max. Frame Rate	PAL	Max. Frame Rate
176 × 120	30	176 × 144	25
352 × 240	30	352 × 288	25
640 × 480	10	640 × 480	8
704 × 480	10	704 × 576	8

NOTE Frame rate (frames per second) is determined by the resolution, image data size (bit rate) and transmission traffic status. The Administrator and users can check the frame rate status in the **FPS Status** on VPort's web homepage.

NOTE A large "Key frame interval" can reduce the bit rate, but will cause the image to be corrupted longer if there is packet loss during transmission.

Video Quality Control

Video Quality Control is used to optimize the bandwidth of the MPEG4 video stream. There are 2 modes for video quality control.

Setting	Description	Default
Fixed bit rate	The administrator can fix the bandwidth to tune the video quality and FPS (frames per second) to the optimum combination. You may choose from the following bandwidths: **55 Kbps**, **70 Kbps**, **90 Kbps**, **105 Kbps**, **115 Kbps**, **180 Kbps**, **240 Kbps**, and **270 Kbps**, or choose **Unlimited** to let the VPort determine the quality and frame rate by itself. The combination of image quality and FPS is determined by the bandwidth. For example, the FPS is slow and the quality is bad at 55 Kbps, and the quality is best at 270 Kbps.	Fixed Quality in good standard
Fixed Quality	The administrator can set the image quality to one of 5 standards: **Medium**, **Standard**, **Good**, **Detailed**, and **Excellent.** VPort will tune the bandwidth and FPS automatically to the optimum combination.	

NOTE The image quality, FPS, and bandwidth are influenced significantly by network throughput, system network bandwidth management, applications VPort runs (such as VMD), how complicated the image is, and the performance of your PC or notebook when displaying images. The administrator should take into consideration all of these variations when designing the video over IP system, and when specifying the requirements for the video system.

Camera Control

VPort supports PTZ (PAN/TILT/ZOOM) motorized camera control via an RS-232 or RS-485 COM port. Before setting up camera control, the administrator should first connect the PTZ camera to the VPort.

Setting	Description	Default
Camera ID	Each PTZ camera has the ID to identify which PTZ camera is in the multi-drop connection. To connect to the PTZ camera, VPort should first identify its ID.	0

Interface mode

Setting	Description	Default
Select the serial interface	The COM port supports 2 serial interfaces, although only one interface can be used at a time. Depending on the interface used by the attached device, administrators must set the **Interface mode** to either RS-232 or RS-485.	RS-485

NOTE The RS-232 interface is used via the DB9 COM port, and RS-485 interface is used via the GPIO. These 2 interfaces cannot be used at the same time.

Port Settings

Setting	Description	Default
Baud rate (bps)	The baud rate specified by the PTZ camera's serial communication specs.	2400
Data bits	The parameters used to define the serial communication.	8
Stop bits		1
Parity bits		None

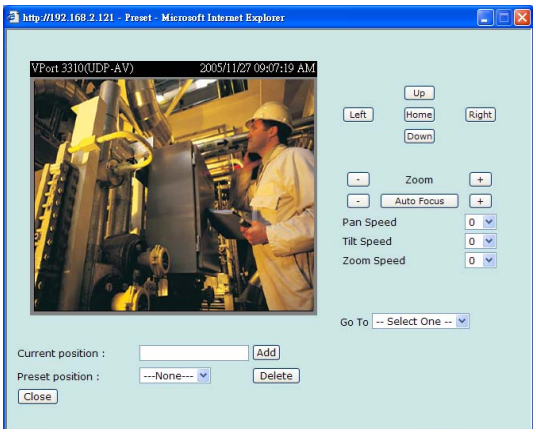
PTZ Camera Drivers

VPort products have some built-in PTZ camera drivers for the convenience of customers to control these popular PTZ cameras directly. Administrators can select the correct PTZ driver in **Select the camera driver** menu. If the attached PTZ camera is not supported by the VPort, administrators can use the **Custom Camera** function to enter the proprietary commands for pan, tilt, zoom, and focus control.

Setting	Description	Default
Select the camera driver	Use the built-in PTZ drivers, including 1. Custom Camera 2. DynaDome/SmartDome (Dynacolor) 3. Emitec 4. Lilin PIH-7x00 (Pending) 5. Pelco D Protocol 6. Samsung/SmartDome 7. Sony Visca 8. Cannon VCC1 9. Cannon VCC3 10. Cannon VCC4	None

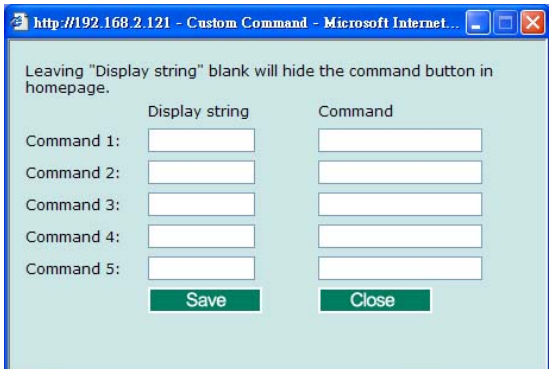
Setting Up a Preset Position

Administrators can use the **Preset Position** function to set up the behavior of the PTZ camera in advance, and then users with camera control privilege can move the camera's lens to a preset position without the need to control the pan, tilt, and zoom buttons on VPort 3310's homepage.



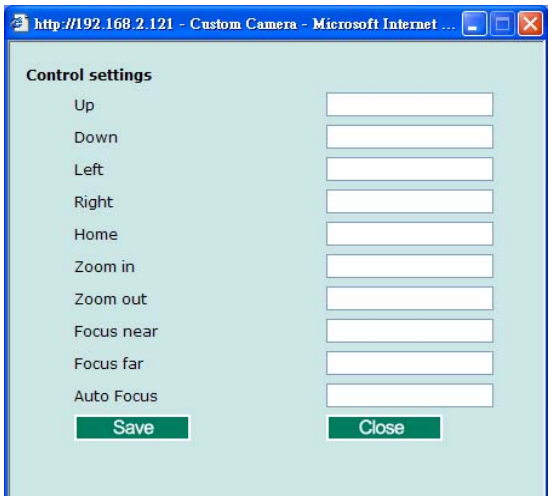
Setting Up Custom Commands

VPort products provide 5 custom commands in addition to the general pan, tilt, zoom, and preset functions. Administrators can click on **Setup Custom Command**s to configure, and refer to the manual enclosed with the attached PTZ camera to set up frequently-used functions. The **Command** should be entered in ASCII format. VPort will translate the commands into binary code and then send the data out through the serial port. For instance, the text string 8101ABCDEF will be translated into five bytes of hexadecimal 81, 01, AB, CD, and EF. The maximum length of a command string is 60, which is equivalent to 30 hexadecimal bytes. The **Display string** is for the text on the command buttons and should be less than 8 characters. If **Custom Camera** is selected, there will be more commands for PTZF that relate to custom camera.



Setting Up Custom Camera

If the PTZ camera's driver is not in the list, the administrator can select the custom camera from the **Select Camera driver** menu to program the PTZ camera with ASCII code**.** A custom camera window will pop up when the **Setup Custom Camera** button is clicked. Input the ASCII code into this window**. Port Settings (Data bits, Stop bits, and Parity bits)** are for the serial communication parameters and **Control Settings** are for programming the **TILT (Move Up, Move Down), PAN (Move Left, Move right), HOME, ZOOM (Zoom in, Zoom out)** and **FOCUS (Focus near, Focus Far)** actions**.**



NOTE The control protocols are available from the PTZ camera's supplier. You will need to get the protocols from the supplier before programming the PTZ camera.

Uploading a PTZ Camera Driver

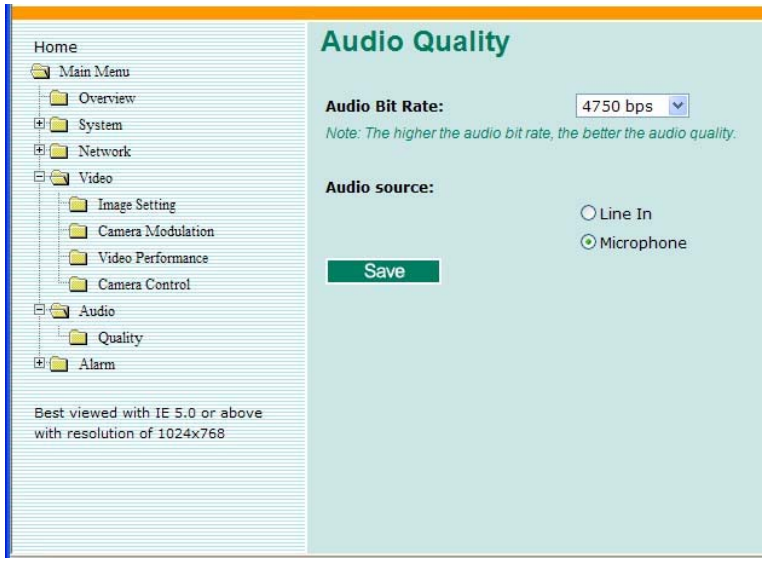
In addition to the PTZ camera drivers and custom camera functions supported by VPort 3310, an alternative user-friendly **Upload a PTZ Camera Driver** function is available for implementing the PTZ camera control. MOXA will release the new PTZ camera drivers to Moxa's website as they become available. Administrators can click on **Browse** to upload the new PTZ camera drivers to VPort 3310.

Audio

Audio Quality

VPort 3310 supports real-time and synchronous video/ audio transmission. Administrators can use bit rate control to determine audio quality**.** The higher the bit rate, the better the quality.

Setting	Description	Default
Audio Bit Rate	There are 8 bit rate levels for audio quality, including **4750 bps, 5150 bps, 5900 bps, 6700 bps, 7400 bps, 7950 bps, 10200 bps** , and **12200 bps.**	4750 bps
Audio Source	For the audio connection, MIC-in (microphone) and Line-in (voice amplifier) are included for convenience. VPort 3310 can auto-sense the audio connection, but administrators also can set these up manually.	Microphone



Alarm

System Alarm

In addition to the LED indicators, three kinds of system alarm are provided by VPort 3310 for notifying the administrator of system operation.

Alarm Type	Triggered Condition	Triggered Action
Power Failure	1. Power 1 failure 2. Power 2 failure	1. Relay 2. Email
Video Loss	Video signal loss	1. Relay 2. Email
Network Disconnected	Network disconnected	Relay

Power Failure Alarm

Setting	Description	Default
Enable power failure alarm	Enable or disable power failure alarm.	Disable

Power 1 Failure/Power 2 Failure

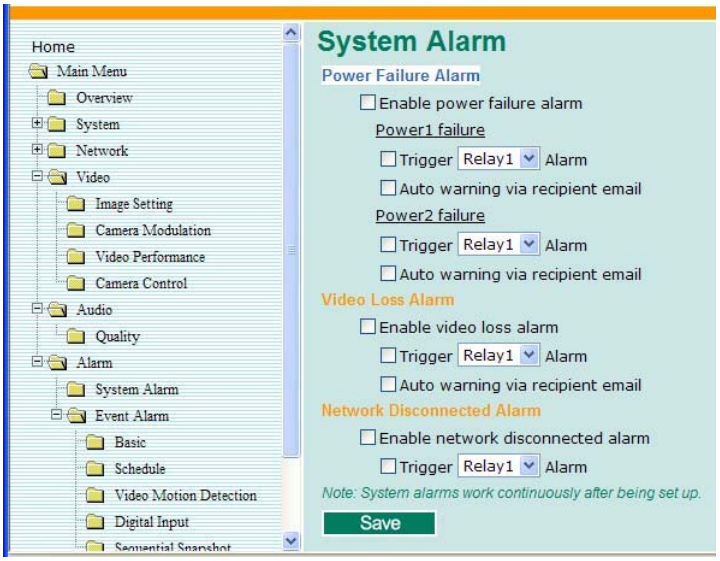
Setting	Description	Default
Trigger Relay alarm	Enable or disable the action in triggering **Relay 1** or **Relay 2** alarms.	Disable
Auto warning via recipient email	Enable or disable the action to send a warning message via recipient's email being set up in **Network/ SMTP Server** configuration page.	Disable

Video Loss Alarm

Setting	Description	Default
Enable video loss alarm	Enable or disable video loss alarm.	Disable
Trigger Relay alarm	Enable or disable the action in triggering **Relay 1** or **Relay 2** alarms.	Disable
Auto warning via recipient email	Enable or disable the action to send a warning message via recipient's email being set up in **Network/ SMTP Server** configuration page.	Disable

Network Disconnected Alarm

Setting	Description	Default
Enable network disconnected alarm	Enable or disable network disconnected alarm.	Disable
Trigger Relay alarm	Enable or disable the action in triggering **Relay 1** or **Relay 2** alarms.	Disable



NOTE Since several alarms can be set up to trigger VPort's relays, the administrator should configure these alarms carefully in case a relay message is read incorrectly.

Event Alarm

Three kinds of event alarm are provided by VPort 3310 for building an intelligent video surveillance system.

Alarm Type	Triggered Condition	Triggered Action
Video Motion Detection (VMD)	1. VMD 1 2. VMD 2 3. VMD 3	1. Relay 2. Email 3. FTP
Digital Inputs	1. DI 1 2. DI 2	1. Relay 2. Email 3. FTP
Sequential Snapshot	Enable sequential snapshot	1. Email 2. FTP

Alarm/Event Alarm/Basic

Alarm Time Interval

Setting	Description	Default
Delay [ ] second(s) before detecting the next alarm	Setup the time interval for each event alarm triggered.	3 seconds (1 to 999 seconds)

NOTE The delay before detecting the next alarm cannot be less than the time needed to take a snapshot after an event (post-event image).

Alarm with Pre and Post snapshot image

Setting	Description	Default
Take snapshot in [ ] seconds(s) before event	Setup the time interval of taking snapshot image before each event alarm triggered.	1 seconds (from 1 to 6 seconds)
Take snapshot in [ ] seconds(s) before event	Enable or disable the function of adding the date and time to the filename.	1 seconds (from 1 to 999 seconds)

NOTE VPort products will take 3 JPEG snapshot images: VPRE.JPG (pre-event), VTRG.JPG (the moment of event) and VPOS.JPG (post-event) for the video channel when the trigger condition is met. Three snapshots of the channel can also be downloaded via FTP or HTTP URL (refer to the "Download Event-triggered Snapshots" section from Chapter 5 for more details).

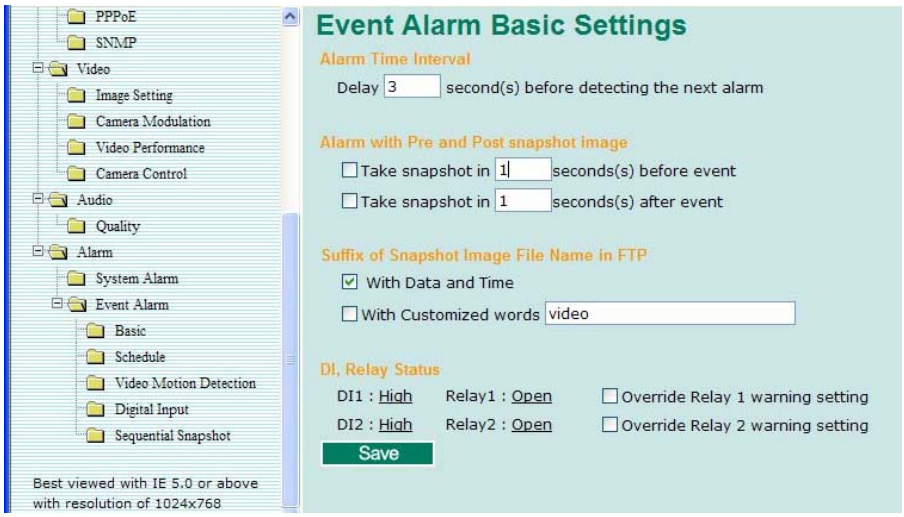
Suffix of Snapshot Image File Name in FTP

The snapshot images can be sent either via email, or via FTP. Administrator can add some suffix to the filename of each JPEG snapshot image to identify them when using FTP to downlaod these snapshot.

Setting	Description	Default
With Data and Time	Enable or disable the function of adding the date and time to the filename.	Enable
With Customized words	Enable or disable the function of adding some additional words to the filename to identify the snapshot image.	Enable

DI, Relay Status

Administrators can check the current DI and Relay status of this VPort in the "DI, Relay Status" section on the "Event Alarm Basic Settings" page. Two options are available to return the relay's status back to the system defaults. To make the function work, check the **Override Relay 1 warning setting** and **Override Relay 2 warning setting** boxes, and then click on **Save**.



NOTE The relays will not be triggered when the **Override Relay 1 warning setting** and **Override Relay 2 warning setting** boxes are checked. Un-check these 2 boxes to ensure that the relays will trigger.

Alarm/Event Alarm/Schedule

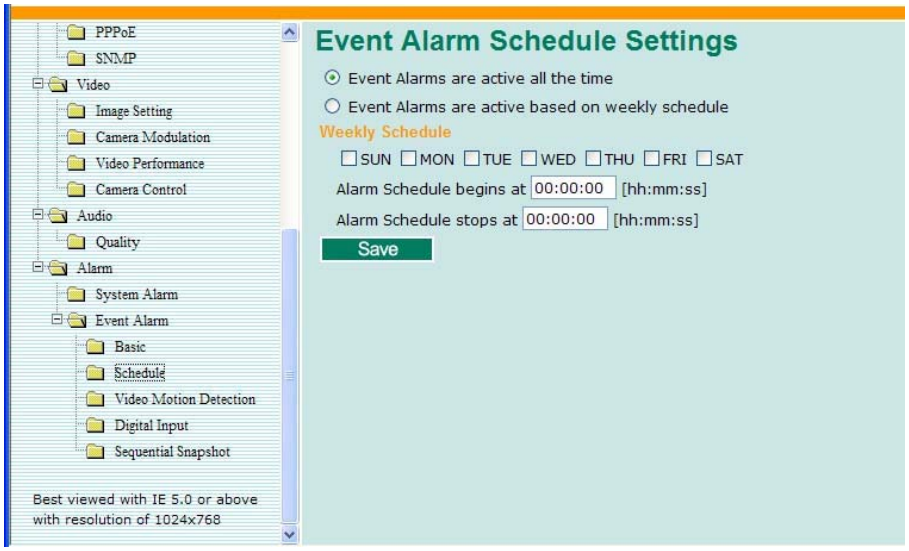
A schedule is provided to set event alarms for daily security applications.

NOTE Either **Event Alarms are active all the time** or **Event Alarms are active based on weekly schedule** must be selected, or the applications described in the following sections will not work properly.

Setting	Description	Default
Event Alarms are active all the time	Select the option "Event Alarms are active all the time"	Event Alarms are active all the time
Event Alarms are on a weekly schedule	Select to operate event alarms on a weekly schedule.	

Weekly Schedule

Setting	Description	Default
☐Sun ☐Mon ☐Tue ☐Wed ☐Thu ☐Fri ☐Sat	Select the weekdays of event alarms' schedule.	None
Alarm Schedule begins at 00:00:00 [hh:mm:ss]	Set the beginning time of event alarms.	00:00:00
Alarm Schedule stops at 00:00:00 [hh:mm:ss]	Setup the stop time of event alarms.	00:00:00

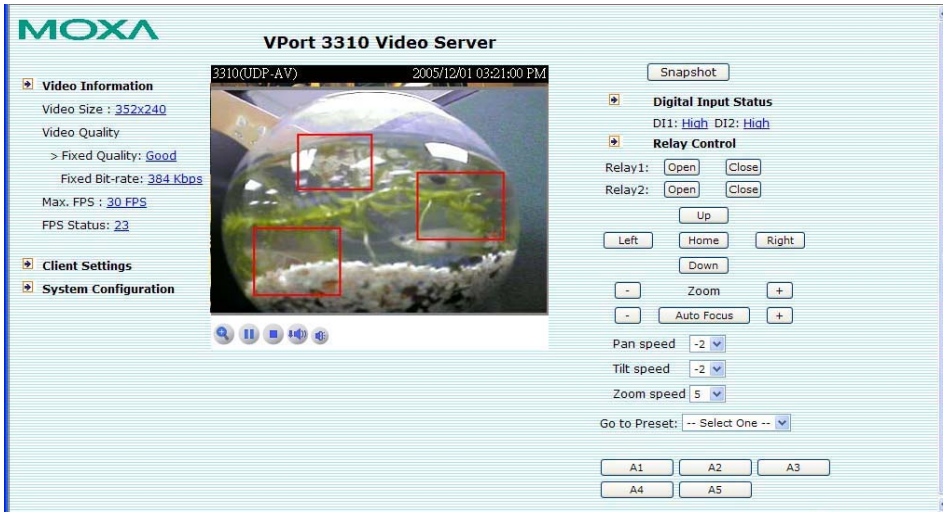


Alarm/Event Alarm/Video Motion Detection

Video Motion Detection (VMD) is an intelligent event alarm for video surveillance network systems. With the 3 area-selectable VMDs and sensitivity/percentage tuning, administrators can easily set up the VMD alarm to be active 24 hours a day, 7 days a week.

Setting	Description	Default
Enable VMD alarm	Enable or disable the VMD alarm.	Disable
Show alert on the image when VMD is triggered	Enable or disable alert for sections of the homepage image on the homepage.	Disable

NOTE Once the **Show alert on the image when VMD is triggered** is enabled, the red frames that appear on the homepage image indicate the size of the VMD window set up by the administrator.



Set up a VMD alarm

Setting	Description	Default
Window Name	The name of each VMD window.	None
Sensitivity	The measurable difference between two sequential images to trigger VMD. Set a larger sensitivity to make it easier for the VMD to be triggered.	0%
Percentage	The minimum size of the image change to trigger the VMD. Set a smaller percentage to make it easier to trigger the VMD.	0%

Trigger Conditions and Actions

Administrators can set up triggers for each VMD, including **Trigger Relay1 alarm**, **Trigger Relay2 alarm**, **Send snapshot image via E-mail**, and **Send snapshot image via FTP**.

How to Set up a VMD alarm

Step 1: **C**heck the ☐ **Enable VMD alarm** box. If the Administrator wants to show the red frame alert on the image on VPort 3310's web homepage, check the ☐ **Show alert on the image when VMD is triggered** box. Click on the **Save** button to save these 2 configurations.

Step 2: Click on the image or the **New** button. A VMD window will pop up. Right click the title bar of this window to move the location of the VMD window, or drag the border to change the window size so that it fits the desired VMD area.

Step 3: Use **Window Name** to assign a name to this VMD window.

Step 4: Set up the **Sensitivity** and **Percentage** parameters by moving the percentage cursor**.**

Step 5: Click on the **Save** button to save the settings**.**

Step 6: To test the VMD condition, check the action of the graphics bar on the left side of the save button. Wave your hand in front of the camera, in the VMD area, and then note which color shows up in the graphics bar. Green means VMD is not triggered. Red means VMD is triggered.

Step 7: Set up the Trigger Conditions and Actions of each VMD, and then click on the **Save** button to save these configurations.

NOTE Video Motion detection is provided as a reference because it is environment-dependent. When the settings are configured to be very sensitive to motion, some triggered events might actually be false alarms, since in fact there is only a tiny difference between sequential images. False alarms can be triggered by the flashing of florescent lights, shifting of shadows, etc.

Alarm/Event Alarm/Digital Input

Two digital inputs are provided by VPort 3310 for linking with alarm detection devices, such as sensors.

Setting	Description	Default
Enable digit input alarm	Enable or disable the digit input alarm.	Disable

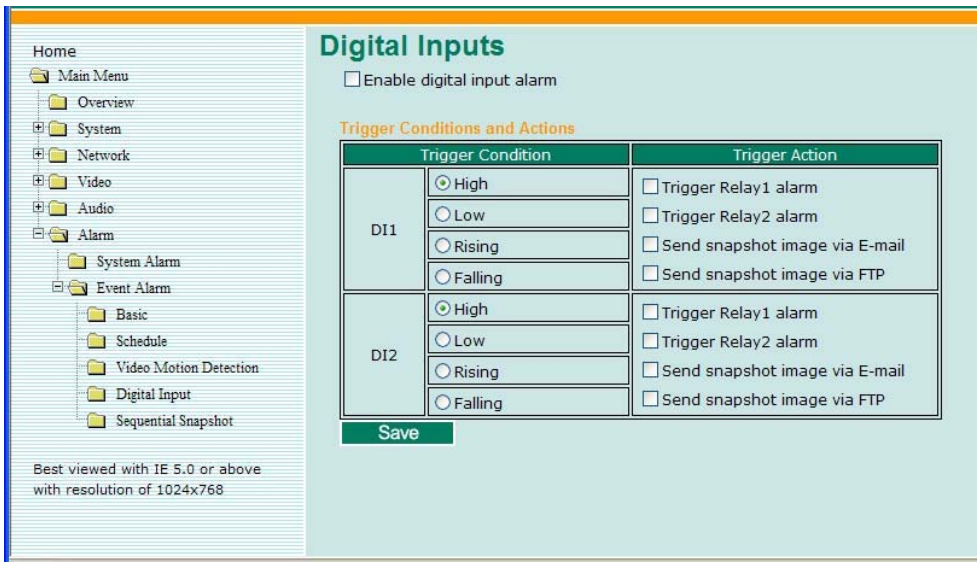
Trigger Conditions

Setting	Description	Default
High	The DI is always in the "High" state after an alarm is detected.	Disable
Low	The DI is always in the "Low" state after an alarm is detected.	Disable
Rising	The DI works from state "Low" to state "High" and then back to state "Low" when an alarm is detected.	Disable
Falling	The DI works from state "High" to state "Low" and then back to state "High" when an alarm is detected.	Disable

NOTE Please refer to Chapter 1 to see the DI specifications.

Trigger Actions

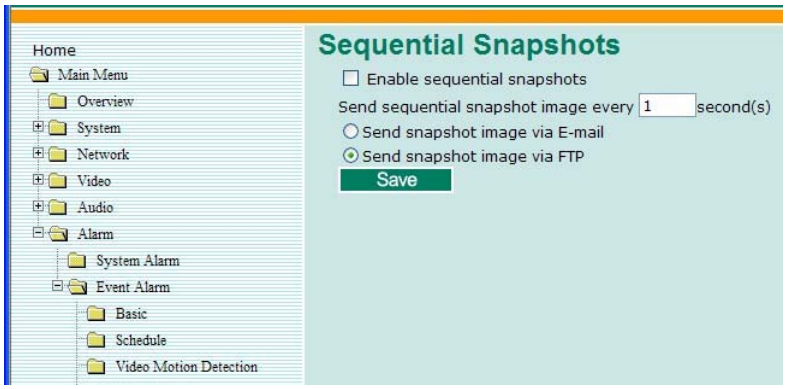
Administrators can set up trigger actions for each DI, including **Trigger Relay1 alarm**, **Trigger Relay2 alarm**, **Send snapshot image via E-mail**, and **Send snapshot image via FTP**.



Alarm/Event Alarm/Sequential Snapshot

With this feature, VPort can upload snapshots periodically to an external E-mail or FTP server as a live video source. Use the **Send sequential snapshot image every** ☐ **seconds** option to set the time interval. The interval can be set to any number from 1 second to 9999 seconds.

Setting	Description	Default
Enable Sequential Snapshots	Enable or disable the Sequential Snapshots.	Disable
Send sequential snapshot image every ☐ seconds	Set the time interval of each snapshot image.	1 second (from 1 second to 99999 seconds)
Send Snapshot image via E-mail	Choose how to send the snapshot images.	Send Snapshot image via FTP
Send Snapshot image via FTP		



System Configuration via FTP

FTP can be used to configure VPort 3310 Video Server much more quickly than configuring from web browser, particularly when configuring multiple Video Servers. To configure a Video Server via FTP, first download the parameter file, CONFIG.INI, customize each field, and then upload the file to the Video Server to install the new settings. To log into the FTP daemon, enter "root" as the user name, and use the same password used when connecting to the web server. The default password of the FTP Server is the MAC address (no dashes, all upper case).

Parameters Available in Config.ini

Group: System

NAME	VALUE	DESCRIPTION
hostname (r/w)	<text string shorter than 40 characters>	host name of server <VPort 3310 Video Server>
date (r/w)	<yyyy/mm/dd>	year, month, date separated by slashes
	<keep>	keep date unchanged
	<auto>	Use NTP to sync date/time automatically
time (r/w)	<hh:mm:ss>	hour, minutes, seconds separated by colons
	<keep>	keep date unchanged
	<auto>	Use NTP to sync date/time automatically
ntp (r/w)	<domain name or IP address>	NTP server <skip to invoke default server>
timezone (r/w)	-12 to 12	time zone, 8 means GMT +8:00 <8>
updateinterval (r/w)	0 to 2592000	0 to Disable automatic time adjustment; a nonzero number indicates the number of seconds between NTP automatic update intervals. <0>
serialnumber (r)	<mac address>	12 character mac address, without hyphens
firmwareversion (r)	<text string shorter than 39 characters>	The version of firmware, including model, company, and internal version number Ex: VS7101-MOXA-0100x
restore (w)	0	Restore the system parameters to default value.
	Positive integer	Restore system parameters to default values and restart the server after <value> seconds.
reset (w)	0 to 65535	Restart the server after <value> seconds.
	-1	Do not restart the server.
do<1~2> (w)	<state>	H: NC connected with COMMON
		L: NO connected with COMMON
di<1~2> (r)	<state>	H: +13 to –30V
		L: -30 to +3V
overridedo<1~2>	0	Enable setting relay
	1	Disable setting relay
supportscriptversion (r)	<text string shorter than 10 characters>	The version of supported script/webpage
scriptversion	<text string shorter than 10 characters >	The maximum version of currently installed script/webpage

language	<text string shorter than 16 characters>	The webpage language Ex: en (English)
webpageversion	<text string shorter than 39 characters>	None
ptzenabled (r)	32-bit integer	Indicate the operations of camera supported
plugincaption (r/w)	0	Hide the caption on plugin
	1	Show the caption on plugin
Description (r)	<text string shorter than 63 characters>	Server description
Contact (r/w)	<text string shorter than 63 characters>	Contact information of the server
Location (r/w)	<text string shorter than 63 characters>	Location information of the server

Group: Security

NAME	VALUE	DESCRIPTION
username_<0-21> (r/w)	<text string shorter than 16 characters>	change user name. The username_0 = root The username_21 = demo <blank>
userpass_<0-21> (r/w)	<text string shorter than 14 characters>	change user's password. The userpass_0 is root's password. The userpass_21 is demo's password <blank>
userattr_<0-21> (r/w)	[dido][|talk][|listen][|camctrl][|conf][do1][do2]	change user's privilege. The privilege can be the combination of dido – Allow DI access do1 – Allow Relay1 access do2 – Allow Relay2 access talk – Allow to talk to server listen – Allow to listen from server camctrl – Allow camera control conf – Allow changing server's configuration view – Allow viewing streaming a/v(check) The userattr_0 = dido | listen | talk | camctrl | do1 | do2 | conf <blank>
usercount (r)	1 to 22	The current account number on the server including root.<1>
snmpuserpass (r/w)	<text string shorter than 14 characters>	change user's password. The snmpuserpass is user's password for SNMP. <blank>

Group: Network

NAME	VALUE	DESCRIPTION
resetip (r/w)(restart)	1	enable getting ipaddress, subnet, router, dns1, dns2 from DHCP server at next reboot
	0	Use preset ipaddress, subnet, router, dns1, dns2

ipaddress (r/w) (restart)	<IP address>	IP address of server <192.168.0.99>
subnet (r/w) (restart)	<IP address>	subnet mask <255.255.255.0>
router (r/w) (restart)	<IP address>	default gateway <blank>
dns1 (r/w) (restart)	<IP address>	primary DNS server <blank>
dns2 (r/w) (restart)	<IP address>	secondary DNS server <blank>
smtp1 (r/w)	<domain name or IP address, string shorter than 40 characters>	primary SMTP server <blank>
mailto1 (r/w)	<string shorter than 80 characters>	mail recipient address <blank>
mailuser1 (r/w)	<text string shorter than 63 characters>	User name of primary smtp server <blank>
mailpass1 (r/w)	<text string shorter than 15 characters>	Password of primary smtp server <blank>
smtp2 (r/w)	<domain name or IP address, string shorter than 40 characters>	secondary SMTP server <blank>
mailto2 (r/w)	<text string shorter than 80 characters>	mail recipient address <blank>
mailuser2 (r/w)	<text string shorter than 63 characters>	User name of secondary smtp server <blank>
mailpass2 (r/w)	<text string shorter than 15 characters>	Password of secondary smtp server <blank>
returnemail1 (r/w)	<text string shorter than 80 characters>	1st return email address <blank>
returnemail2 (r/w)	<text string shorter than 80 characters>	2nd return email address <blank>
localftpport (r/w)	<positive number less than 65535>	FTP port <21>
ftp1 (r/w)	<domain name or IP address, string shorter than 40 characters >	primary FTP server <blank>
ftpport1 (r/w)	<positive number less than 65535>	primary FTP port <21>
ftpuser1 (r/w)	<text string shorter than 63 characters>	user name for primary FTP server <blank>
ftppass1 (r/w)	<text string shorter than 15 characters>	password for primary FTP server <blank>
ftpfolder1 (r/w)	<text string shorter than 40 characters>	upload folder in primary FTP server <blank>
ftppasvmode1 (r/w)	1	Enable passive mode of primary FTP server
	0	Disable passive mode of primary FTP server
ftp2 (r/w)	<domain name or IP address, string shorter than 40 characters>	secondary FTP server
ftpport2 (r/w)	<positive number less than 65535>	secondary FTP port <21>

ftpuser2 (r/w)	<text string shorter than 63 characters>	user name for secondary FTP server <blank>
ftppass2 (r/w)	<text string shorter than 15 characters>	password for secondary FTP server <blank>
ftpfolder2 (r/w)	<text string shorter than 40 characters>	upload folder in secondary FTP server <blank>
ftppasvmode2 (r/w)	1	Enable passive mode of primary FTP server
	0	Disable passive mode of primary FTP server
httpport (r/w) (restart)	<positive number less than 65535>	HTTP port <80>
rtspport (r/w) (restart)	<positive number less than 65535>	RTSP port <554>
accessname (r/w) (restart)	<text string shorter than 32 characters>	Name for accessing RTSP a/v streaming <live.sdp>
networktype	0	PPPoE is disabled
	1	Use PPPoE
pppoeuser	<text string shorter than 63 characters>	The user name for PPPoE connection
pppoepass	<text string shorter than 63 characters>	The password for PPPoE connection

Group: IPFilter (Assessible IP)

NAME	VALUE	DESCRIPTION
allowip_<0-9> (r/w)	1.0.0.0 to 255.255.255.255	Allowed RTSP connection IP address <blank>
allowmask_<0-9> (r/w)	1.0.0.0 to 255.255.255.255	Allowed RTSP connection IP mask <blank>
allowenable	0	Enable IP filter
	1	Disable IP filter

Group: Video

NAME	VALUE	DESCRIPTION
text (r/w)	<text string shorter than 14 characters>	enclosed caption <blank>
codectype (r/w)	0	MPEG4
keyinterval (r/w)	1, 3, 5, 10, 30, 60, 90, 120	Key frame interval <120>
size (r/w)	1	half
	2	half x 2
	3	normal
	4	normal x 2
	5	double
color (r/w)	0	Monochrome(B/W)
	1	color

quality (r/w)	0	fix bit rate
	1	fix quantization
quant (r/w)	1	lowest quality of video
	2	lower quality of video
	3	normal quality of video
	4	higher quality of video
	5	highest quality of video
bitrate (r/w)	64000	set bit rate to 64 Kbps
	128000	set bit rate to 128 Kbps
	256000	set bit rate to 256 Kbps
	384000	set bit rate to 384 Kbps
	512000	set bit rate to 512 Kbps
	768000	set bit rate to 768 Kbps
	1000000	set bit rate to 1000 Kbps
	1200000	set bit rate to 1200 Kbps
maxframe (r/w)	1	set maximum frame rate to 1 fps
	2	set maximum frame rate to 2 fps
	3	set maximum frame rate to 3 fps
	5	set maximum frame rate to 5 fps
	10	set maximum frame rate to 10 fps
	15	set maximum frame rate to 15 fps
	20	set maximum frame rate to 20 fps
	25	set maximum frame rate to 25 fps
	30 (for NTSC only)	set maximum frame rate to 30 fps
modulation (r/w) (restart)	0	NTSC
	1	PAL
	2	AUTO
actualmodulation (r)	0	NTSC
	1	PAL
flip (r/w)	1	flip image
	0	normal image
mirror (r/w)	1	mirror image
	0	normal image
imprinttimestamp (r/w)	1	Overlay text and time stamp on video; in QCIF, only time stamp is overlayed
	0	Do not overlay text and time stamp on video

Group: Audio

NAME	VALUE	DESCRIPTION
bitrate (r/w)	4750	4750 Kbps
	5150	5150 Kbps
	5900	5900 Kbps
	6700	6700 Kbps
	7400	7400 Kbps
	7950	7950 Kbps
	10200	10200 Kbps
	12200	12200 Kbps
source (r/w)	0	Use external microphone in
	1	Use line-in

Group: Image

NAME	VALUE	DESCRIPTION
brightness (r/w)	<-5 to 5>	Adjust brightness of image according to mode settings. **<0>**
saturation (r/w)	<-5 to 5>	Adjust saturation of image according to mode settings. **<0>**
contrast (r/w)	<-5 to 5>	Adjust contrast of image according to mode settings. **<0>**
hue (r/w)	<-5 to 5>	Adjust hue of image according to mode settings. **<0>**
mode (w)	Preview	Apply the parameter of image but not save
	Restore	Restore the last saved image parameters
	Save	Directly save the adjust image parameters

Group: Motion

NAME	VALUE	DESCRIPTION
enabled (r/w)	0	disable motion detection
	1	enable motion detection
alertonvideo (r/w)	0	Do not display alert window on streaming video
	1	Display alert window on streaming video
winenabled_<1-3> (r/w)	0	disable motion window #1
	1	enable motion window #1
winname_<1-3> (r/w)	<text string shorter than 14 characters >	name of motion window #1 <blank>
winleft_<1-3> (r/w)	*0 to 352 for CCD* *0 to 320 for CMOS*	Left coordinate of window position. <0>
wintop_<1-3> (r/w)	*0 to 288 for PAL* *0 to 240 for NTSC & CMOS*	Top coordinate of window position. <0>

winwidth_<1-3> (r/w)	*0 to 352 for CCD* 0 to 320 for CMOS	Width of motion detection window. <0>
winheight_<1-3> (r/w)	*0 to 288 for PAL* *0 to 240 for* NTSC & CMOS	Height of motion detection window. <0>
winobjsize_<1-3> (r/w)	*0 to 100*	Percent of motion detection window <0>
winsensitivity_<1-3> (r/w)	*0 to 100*	Sensitivity of motion detection window <0>
update (w)	*1*	Update the above motion detection settings to take effect

Group: DDNS

NAME	VALUE	DESCRIPTION
enable (r/w)	0, 1	Enable or disable the dynamic dns. <0>
provider (r/w)	1 to 4	dyndns.org (dynamic) dyndns.org (custom) tzo.com dhs.org <1>
hostname (r/w)	Text string shorter than 127 characters.	Your dynamic hostname. <blank>
usernameemail (r/w)	Text string shorter than 63 characters.	Your user or email to login ddns service provider <blank>
passwordkey (r/w)	Text string shorter than 20 characters.	Your password or key to login ddns service provider <blank>
update (w)	0, 1	Update the above ddns settings to take effect

Group: MULTICAST

NAME	VALUE	DESCRIPTION
ipaddress (r/w)(restart)	<IP address>	Multicast IP address <239.128.0.99> The valid range of multicast IP is from 224.0.0.0 to 239.255.255.255
videoport (r/w)(restart)	1 to 65536	Destination multicast port of video <5556>
audioport (r/w)(restart)	1 to 65536	Destination multicast port of audio <5558>
ttl (r/w)	1 to 255	Time to live of multicast packets <15>
enablem (r/w)(restart)	0, 1	Enable or disable always multicast <0>

Group: UPNP

NAME	VALUE	DESCRIPTION
enable (r/w)	0, 1	Enable or disable the UPNP service. <1>

Group: SNMP

NAME	VALUE	DESCRIPTION
versions (r/w) (restart)	1	V1, V2c, V3
	2	V1, V2c (default)
	3	V3 only
rocomm (r/w) (restart)	<text string shorter than 14 characters>	ID for V1, V2c Read Community <public>
rwcomm (r/w) (restart)	<text string shorter than 14 characters>	ID for V1, V2c Write/Read Community <private>
adminauthtype (r/w) (restart)	0	No-Auth
	1	MD5
	2	SHA
admindpvcy (r/w) (restart)	<text string shorter than 30 characters>	Admin data encryption key if needed <blank>
enableadpvcy (r/w) (restart)	0, 1	Enable the admin data encryption key <0>
userauthtype (r/w) (restart)	0	No-Auth
	1	MD5
	2	SHA
userdpvcy (r/w) (restart)	<text string shorter than 30 characters>	User data encryption key if needed <blank>
enableudpvcy (r/w) (restart)	0, 1	Enable the user data encryption key <0>
trapserver (r/w) (restart)	<domain name or IP address>	Trap server name or IP address for actively sending message to SNMP manager <blank>
trapcomm (r/w) (restart)	<text string shorter than 14 characters>	ID for Trap Community <public>
Objectid (r) (restart)	<text string shorter than 30 characters>	Private enterprise number for SNMP <enterprise.8691>

Group: App

NAME	VALUE	DESCRIPTION
scriptname (r/w)	<text string shorter than 255 characters>	File name of script <script.vssx>
enablescript (r/w)	0	Disable script
	1	Enable script

Group: CAMCTRL

NAME	VALUE	DESCRIPTION
panspeed (r/w)	-5 to 5	Pan speed <0>
tiltspeed (r/w)	-5 to 5	Tilt speed <0>
autospeed (r/w)	-5 to 5	Auto pan speed <0>
axisx (r)	-104 to 104	X coordinate of camera position <0>
axisy (r)	-15 to 28	Y coordinate of camera position <0>
dwelling (r/w)	0 to 9999	Time to dwell when patrolling <1>
presetname_<0-19> (r/w)	Text string shorter than 40 characters.	The name of preset location <blank>
presetpan_<0-19> (r/w)	Integer	pan coordinate of preset location. <0>
presettilt_<0-19> (r/w)	Integer	tilt coordinate of preset location. <0>
presetzoom_ <0-19> (r/w)	Integer	zoom coordinate of preset location. <0>
serial	0	UART1
	1	UART2
cameraid	Integer	The camera ID to control
isptz	0	PTZ camera
	1	Non-PTZ camera

Group: Serial

NAME	VALUE	DESCRIPTION
baudrate (r/w)	110	110 bps
	300	300 bps
	600	600 bps
	1200	1200 bps
	2400	2400 bps
	3600	3600 bps
	4800	4800 bps
	7200	7200 bps
	9600	9600 bps
	19200	19200 bps
	38400	38400 bps
	57600	57600 bps
	115200	115200 bps

databit (r/w)	5	5 bits
	6	6 bits
	7	7 bits
	8	8 bits
paritybit (r/w)	0	None
	1	Odd
	2	Even
stopbit (r/w)	1	1 bit
	2	1.5 bits (databits : 5) 2 bits (databits: 6, 7, 8)
uartmode (r/w)	0	RS232
	1	RS485
customcmd_<0~9>	<Text string shorter than 61 characters.>	Customer command to control camera
speedlinkname_<0~4>	Text string shorter than 9 characters.	Speed link command name
speedlinkcmd_<0~4>	Text string shorter than 61 characters.	Speed link command to control camera
ptzdriver	128	None
	129	Custom camera
	Positive integer	Other camera

5

URL (CGI) Commands

For customers who already have their own web site or web control application, VPort products can be easily integrated through convenient URLs. This section lists the commands in URL format corresponding to the basic functions of VPort products.

The following topics are covered in this chapter:

- **Overview**
- **Style Convention**
- **General CGI URL Syntax and Parameters**
- **Get Server Parameter Values**
- **Set Server Parameter Values**
- **Drive the Digital (Relay) Output**
- **Query Status of the Digital Input**
- **Query Status of the Digital (Relay) Onput**
- **Capture Single Snapshot**
- **Account Management**
- **System Logs**
- **Configuration File**
- **Camera Control**
- **Recall**
- **System Information**
- **Preset Locations**

Overview

This section specifies the external HTTP based application programming interface. The HTTP based VPort's interface provides the functionality to request a single image, to control camera functions (PTZ, output relay etc.) and to get and set internal parameter values. The image and CGI-requests are handled by the built in Web server.

Style Convention

In URL syntax and in descriptions of CGI parameters, a text in italic within angle brackets denotes a content that is to be replaced with either a value or a string. When replacing the text string also the angle brackets shall be replaced. An example of this is the description of the name for the server, denoted with <servername> in the URL syntax description below, that is replaced with the string myserver in the URL syntax example, also below.

URL syntax' are written with the "**Syntax:**" word written in bold face followed by a box with the referred syntax as seen below. The name of the server is written as <servername>. This is intended to be replaced with the name of the actual server. This can either be a name, e.g., "mywebcam" or "thecam.adomain.net" or the associated IP number for the server, e.g., 192.168.0.220.

Syntax:

```
http://<servername>/cgi-bin/video.jpg
```

Description of returned data is written with "**Return:**" in bold face followed by the returned data in a box. All data returned as HTTP formatted, i.e., starting with the string HTTP is line separated with a Carriage Return and Line Feed (CRLF) printed as \r\n.

Return:

```
HTTP/1.0 <HTTP code> <HTTP text>\r\n
```

URL syntax examples are written with "**Example:**" in bold face followed by a short description and a light grey box with the example.

Example: request a single snapshot image

```
http://mywebserver/cgi-bin/video.jpg
```

General CGI URL Syntax and Parameters

CGI parameters are written in lower-case and as one word without any underscores or other separators. When the CGI request includes internal camera parameters, the internal parameters must be written exactly as they are named in the camera or video server. The CGIs are organized in function related directories under the cgi-bin directory. The file extension of the CGI is required.

Syntax:

```
http://<servername>/cgi-bin/<subdir>[/<subdir>...]/<cgi>.<ext>
[?<parameter>=<value>[&<parameter>=<value>...]]
```

Example: Setting digital output #1 to high

```
http://mywebserver/cgi-bin/setparam.cgi?do1=h
```

Get Server Parameter Values

Note: This request require administrator access

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/getparam.cgi?[<parameter>]
[&<parameter>…]
```

where the <*parameter*> should be <*group*>[_<*name*>] or <*group*>[.<*name*>]

If you do not specify the any parameters, all the parameters on the server will be returned. If you specify only <*group*>, the parameters of related group will be returned.

When query parameter values, the current parameter value are returned. Successful control requests returns parameter pairs as follows.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<parameter pair>
```

where <parameter pair> is
<parameter>=<value>\r\n
[<parameter pair>]
<length> is the actual length of content.

Example: request IP address and it's response

Request:

```
http://192.168.0.123/cgi-bin/admin/getparam.cgi?network_ipaddress
```

Response:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network.ipaddress=192.168.0.123\r\n
```

Set Server Parameter Values

Note: This request require administrator access

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/setparam.cgi?
[nosync=<value>&]<parameter>=<value>
[&<parameter>=<value>…][&return=<return page>]
```

Parameter	Value	Description
NOSYNC	*0, 1*	Specifies that there should be no sync (write) of the corresponding configuration file on flash. If parameter is omitted, a sync write will occur. **(Note: this parameter must be put at begin of parameter list)**
<GROUP>_<NAME>	value to assigned	Assign <*value*> to the parameter <*group*>_<*name*>.
RETURN	<*return page*>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according the current path. If you omit this parameter, it will redirect to an empty page. **(Note: The return page can be a general HTML file(.htm, .html) or a Vivotek server script executable (.vspx) file. It can not be a CGI command. It can not have any extra parameters. This parameter must be put at end of parameter list)**

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<parameter pair>
```

where <parameter pair>
is <parameter>=<value>\r\n
[<parameter pair>]

Note: Only the parameters that you set and readable will be returned.

Example: Set the IP address of server to 192.168.0.123

Request:

```
http://myserver/cgi-bin/admin/setparam.cgi?Network_IPAddress=192.168.0.123
```

Response:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network.ipaddress=192.168.0.123\r\n
```

Drive the Digital (Relay) Output

Note: This request requires the privilege of I/O access control.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/setdo.cgi?do1=<state>[&do2=<state>]
[&return=<return page>]
```

Where state is H, L. H means NC (normal close) connected with COMMON and L means NO (normal open) connected with COMMON. The number of DO dependents on the server type.

Parameter	Value	Description
DO<NUM>	<state>	H – NC connected with COMMON
		L – NO connected with COMMON
RETURN	<*return page*>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according the the current path. If you omit this parameter, it will redirect to an empty page.

Example: Drive the digital output 1 to high and redirect to an empty page

```
http://myserver/cgi-bin/setdo.cgi?do1=H
```

Query Status of the Digital Input

Note: This request requires the privilege of I/O access control.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/getdi.cgi?[di1][&di2]
```

If no parameter is specified, all the status of digital input will be returned.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <length>\r\n
\r\n
[di1=<state>]\r\n
[di2=<state>]\r\n
```

where <*state*> can be H or L.

Example: Query the status of digital input 1

Request:

```
http://myserver/cgi-bin/getdi.cgi?di1
```

Response:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: 7\r\n
\r\n
di1=H\r\n
```

Query Status of the Digital (Relay) Output

Note: This request requires the privilege of I/O access control.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/getdo.cgi?[do1][&do2]
```

If no parameter is specified, all the status of digital output will be returned.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <length>\r\n
\r\n
[do1=<state>]\r\n
[do2=<state>]\r\n
```

where <*state*> can be H or L.

Example: Query the status of digital output 1

Request:

```
http://myserver/cgi-bin/getdo.cgi?di1
```

Response:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: 7\r\n
\r\n
do1=H\r\n
```

Capture Single Snapshot

Note: This request require normal user privilege

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/video.jpg
```

Server will return the most up-to-date snapshot in JPEG format. The size and quality of image will be set according to the JPEG settings on the server.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: image/jpeg\r\n
[Content-Length: <image size>\r\n]

<binary JPEG image data>
```

Account Management

Note: This request requires administrator privilege

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/editaccount.cgi?
method=<value>&username=<name>[&userpass=<value>]
[&privilege=<value>]
[&privilege=<value>][…][&return=<return page>]
```

Parameter	Value	Description
method	add	Add an account to server. When using this method, "username" field is necessary. It will use default value of other fields if not specified.
	delete	Remove an account from server. When using this method, "username" field is necessary, and others are ignored.
	edit	Modify the account password and privilege. When using this method, "username" field is necessary, and other fields are optional. If not specified, it will keep original settings.
username	<name>	The name of user to add, delete or edit
userpass	<value>	The password of new user to add or that of old user to modify. The default value is an empty string.
privilege	<value>	The privilege of user to add or to modify. The privilege can be the addition of the following values. Ex: A user with DI/DO access and listen privilege can be assigned privilege as **privilege=dido&privilege=listen**.
	dido	DI access privilege (for Moxa Vport3310) DI/DO access privilege (for other servers)
	do1	DO1 access privilege
	do2	DO2 access privilege
	listen	listen privilege
	talk	talk privilege
	camctrl	camera control privilege (support only on PT(Z) version)
	conf	configuration privilege
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according the the current path. If you omit this parameter, it will redirect to an empty page.

System Logs

Note: This request require administrator privilege

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/syslog.cgi
```

Server will return the up-to-date system log.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <syslog length>\r\n
\r\n
<system log information>\r\n
```

Configuration File

Note: This request requires administrator privilege

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/configfile.cgi
```

Server will return the up-to-date configuration file.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <configuration file length>\r\n
\r\n
<configuration data>\r\n
```

Camera Control

Note: This request requires camera control access privilege

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/camctrl.cgi?
[move=<value>][&speedpan=<value>][&speedtilt=<value>]
[&return=<return page>]
```

Parameter	Value	Description
move	home	Move to camera to home position
	up	Move camera up
	down	Move camera down
	left	Move camera left
	right	Move camera right
speedpan	-5 ~ 5	Set the pan speed
speedtilt	-5 ~ 5	Set the tilt speed
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

Recall

Note: This request requires camera control access privilege

Method: GET

Syntax:

```
http://<servername>/cgi-bin/recall.cgi?
recall=<value>[&return=<return page>]
```

Parameter	Value	Description
recall	Text string less than 30 characters	One of the present positions to recall.
return	<*return page*>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

System Information

Note: This request requires normal user privilege

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/sysinfo.cgi
```

Server will return the system information.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <system information length>\r\n
\r\n
Model=<model name of server>\r\n
HostName=<host name of server>\r\n
Location=<video on text of server>\r\n
[Preset<0>=<first preset location>\r\n]
[Preset<1>=<second preset location>\r\n]
[...]
PTZEnabled=<PTZ status>\r\n
Event=<value>\r\n
RTSPPort=<value>\r\n
CameraNumber=<value>\r\n
UartNumber=<value>\r\n
DINumber=<value>\r\n
DONumber=<value>\r\n
VideoCodec=<value>\r\n
AudioCodec=<value>\r\n
MotionDetectionMethod=<value>\r\n
StreamingProtocol=<value>\r\n
```

Parameter	Value	Description
Model	system.firmwareversion	Model name of server.
HostName	system.hostname	Host name of server
(one channel) Location (multichannel) Location<0~>	*(one channel)* *video.text* *(multichannel)* *video.text (first channel)* *video<1~>.text (other channels)*	Text on video, representation the location of video
Event	*0*	
	1	*support motion detection/dido/video loss information in video bitstream*
RTSPPort	*network.rtspport*	Port number of RTSP
(one channel) Preset<0~> (multichannel) Location<0~>_<0~>	*(one channel)* *camctrl.presetname_<0~>* *(multichannel)* *camctrl.presetname_<0~> (first channel)* *camctrl<1~>.presetname_<0~> (other channels)*	Preset locations of PTZ camera
(one channel) PTZEnabled (multichannel) PTZEnabled<0~>	An 32-bits integer, each bit can be set separately as follows: Bit 0 => Support camera control function 0(not support), 1(support) Bit 1 => **Build-in** or **external** camera. 0(external), 1(build-in) Bit 2 => Support **pan** operation. 0(not support), 1(support) Bit 3 => Support **tilt** operation. 0(not support), 1(support) Bit 4 => Support **zoom** operation. 0(not support), 1(support) *Bit 5 => Support **focus** operation. 0(not support), 1(support)*	
CameraNumber	1~16	Number of camera supported
UartNumber	1~16	Number of uart supported
DINumber	1~16	Number of DI supported
DONumber	1~16	Number of DO supported
VideoCodec	<codecname>,<codecname>,… Available video codec name: MJPEG => Motion JPEG MP4SHM => MPEG4 short header mode MP4SP => MPEG4 simple profile	Supported video codec name separated by comma.
AudioCodec	<codecname>,<codecname>,… Available audio codec name: G7221 => G.722.1 G729A => G.729A GAMR => GSM AMR AAC => AAC	Supported audio codec name separated by comma.

MotionDetectionMethod	1 => full screen motion detection 3 => three windows motion detection	An integer to indicate the motion detection method
StreamingProtocol	<protocolname>, <protocolname>,… RTSP_RTP_UDP => RTP over UDP RTSP_RTP_TCP => RTP over RTSP RTSP_RTP_HTTP => RTSP, RTP over HTTP RTSP_RTP_MCAST => Backbone multicast RTP_MCAST => Scalable multicast	Supported streaming protocol

Preset Locations

Note: This request requires administrator access privilege

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/preset.cgi?
[addpos=<value>][&delpos=<value>][&return=<return page>]
```

Parameter	Value	Description
addpos	<Text string less than 30 characters>	Add one preset location to preset list.
delpos	<Text string less than 30 characters>	Delete preset location from preset list.
return	*<return page>*	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

A

Frequently Asked Questions

Q: What if I forget my password?

A: Every access to the Video Server needs authentication. If you are one of the managed users, you need to ask the administrator for the password. If you are the administrator, there is no way to recover the root password. The only way to regain access to Video Server is to utilize the default setting button on the rear panel to restore the factory settings (see p. 1-7 for details).

Q: Why can't I see video from the Video Server after it has been authenticated?

A: There are many possible scenarios:

1. If you have just installed the Video Server and are unable to see the video, check the video modulation on the Configuration page.
2. If the Video Server is installed correctly and you are accessing the Video Server for the first time using Internet Explorer, adjust the security level of Internet Explorer to allow installation of plug-ins.
3. If the problem still exists, the number of users accessing the Video Server at the same time may exceed the maximum that the system allows.

Q: What is the plug-in for?

A: The plug-in provided by Video Server is used to display motion pictures on versions of Internet Explorer that do not support server push technology. If your system does not allow installation of any plug-in software, the security level of the web browser may need to be lowered. It is recommended that you consult the network supervisor in your office before adjusting the security level.

Q: Why is the timestamp different from the system time of my PC or notebook?

A: The timestamp is based on the system time of Video Server. It is maintained by an internal real-time clock, and automatically synchronizes with the time server if Video Server is connected to the Internet and the function is enabled. Differences of several hours may result from the time zone setting.

Q: Why doesn't the image refresh regularly?

A: This may be due to the time taken for storing snapshots into memory when events occur.

Q. How does the Video Server detect supported PTZ cameras automatically?

A. If a camera is not detected, the Video Server will monitor the CTS of the camera control cable continuously. As long as the CTS is detected, the Video Server will try to handshake with supported cameras until a supported camera is found. Camera detection will cease once a PTZ

camera is recognized.

Q: How many users are allowed to access Video Server at the same time?

A: Basically, there is no limitation. However the video quality also depends on the network bandwidth. To achieve the best effect, the Video Server will allow 20 users to be connected. It is recommended to build another web server to host a large quantity of users by retrieving images from the Video Server periodically.

Q: What is Video Server's video rate?

A: The MPEG4 codec can process 30 frames per second internally. However the total performance is subject to many coefficients as follows:

1. Network throughput.
2. Bandwidth share.
3. Number of users.
4. The complicated objects in view results in larger image file.
5. The level of your PC or notebook which is responsible for displaying images.

In general, the transfer rate for a general local network environment can achieve over 200 kilobytes per second and approximately 10 to 20 pictures of a normal environment per second.

Q: How can I keep the Video Server as private as possible?

A: The Video Server is designed for surveillance purposes and has many flexible interfaces. The user authentication and special confirmation when installing can keep the Video Server from unauthorized access. You may also change the HTTP port to a non-public number. Check the system log to examine any abnormal activities and trace the origins.

Q: I have a PTZ camera that is not on the support list. How can I control it?

A: Video Server provides a custom camera command interface to control cameras that are not supported. The details are described in this manual. Be sure that the COM port settings are applied to the camera specifications. The camera control cable included is shown in the package contents. Prepare your own cable if necessary. The general PTZ command is composed of one start command and one stop command. When editing both commands in the edit box of the configuration page, use comma(s) to separate commands. Each comma represents 200 milliseconds. If the user has some serial control device other than the PTZ camera, the special URL is provided to send the desired commands. For quick access, integrate the URL to another homepage on your own web server.

Q: How fast will Video Server check the status of digital inputs?

A: The Video Server will check input status in less than half a second. However, to avoid repeatedly checking conditions too often and to allow the devices connected to digital outputs to function properly, the Video Server will delay 3 seconds by default after each condition matches. Users may change it according to specific applications. During this period, any condition will be ignored.

Q: Why can't I access the Video Server when I set up some options in the application?

A: When the Video Server is triggered by events; snapshots will take more time to write to memory. If the events occur too often, the system will always be busy storing images. It is recommended to use sequential mode or an external recorder program to record motion pictures if the event is frequent. If you prefer to retrieve images via FTP, the value could be smaller since FTP responds quicker than the Web does. Once the system is too busy to

configure, use the restore factory default and reset button to save the system.

Q: I tried connecting my black-and-white and color cameras with the Video Server but the image is not good.

A: Although the Video Server allows users to choose color or black-and-white images for each camera, hybrid camera types may increase video processing time and reduce system performance.

Q: The image is not clear enough. Is anything broken?

A: The lens can be focused by rotating the outer ring. Rotate it clockwise or counter-clockwise to focus near or far.

B

Settings of Supported PTZ Cameras

Since the COM port settings can be adjusted to other than the default settings, check the correct default settings for the attached camera.

Camera model	Baud rate	Data bits	Stop bit	Parity bit
Sony VISCA	9600	8	1	None
Canon VC-C1	9600	8	2	None
Canon VC-C3	9600	8	2	None
Canon VC-C4	9600	8	1	None
Pelco D protocol	2400	8	1	None
DynaDome/SmartDome	9600	8	1	None

C

Time Zone Table

The hour offsets for different time zones are shown below. You will need this information when setting the time zone in automatic date/time synchronization. GMT stands for Greenwich Mean Time, which is the global time that all time zones are measured from.

(GMT-12:00) International Date Line West
(GMT-11:00) Midway Island, Samoa
(GMT-10:00) Hawaii
(GMT-09:00) Alaska
(GMT-08:00) Pacific Time (US & Canada), Tijuana
(GMT-07:00) Arizona
(GMT-07:00) Chihuahua, La Paz, Mazatlan
(GMT-07:00) Mountain Time (US & Canada)
(GMT-06:00) Central America
(GMT-06:00) Central Time (US & Canada)
(GMT-06:00) Guadalajara, Mexico City, Monterrey
(GMT-06:00) Saskatchewan
(GMT-05:00) Bogota, Lima, Quito
(GMT-05:00) Eastern Time (US & Canada)
(GMT-05:00) Indiana (East)
(GMT-04:00) Atlantic Time (Canada)
(GMT-04:00) Caracas, La Paz
(GMT-04:00) Santiago
(GMT-03:30) Newfoundland
(GMT-03:00) Brasilia
(GMT-03:00) Buenos Aires, Georgetown
(GMT-03:00) Greenland
(GMT-02:00) Mid-Atlantic
(GMT-01:00) Azores
(GMT-01:00) Cape Verde Is.
(GMT) Casablanca, Monrovia
(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
(GMT+01:00) Amsterdam, Berlin, Bern, Stockholm, Vienna
(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
(GMT+01:00) Brussels, Copenhagen, Madrid, Paris
(GMT+01:00) Sarajevo, Skopje, Warsaw, Zagreb
(GMT+01:00) West Central Africa
(GMT+02:00) Athens, Istanbul, Minsk
(GMT+02:00) Bucharest
(GMT+02:00) Cairo

(GMT+02:00) Harare, Pretoria
(GMT+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius
(GMT+02:00) Jerusalem
(GMT+03:00) Baghdad
(GMT+03:00) Kuwait, Riyadh
(GMT+03:00) Moscow, St. Petersburg, Volgograd
(GMT+03:00) Nairobi
(GMT+03:30) Tehran
(GMT+04:00) Abu Dhabi, Muscat
(GMT+04:00) Baku, Tbilisi, Yerevan
(GMT+04:30) Kabul
(GMT+05:00) Ekaterinburg
(GMT+05:00) Islamabad, Karachi, Tashkent
(GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi
(GMT+05:45) Kathmandu
(GMT+06:00) Almaty, Novosibirsk
(GMT+06:00) Astana, Dhaka
(GMT+06:00) Sri Jayawardenepura
(GMT+06:30) Rangoon
(GMT+07:00) Bangkok, Hanoi, Jakarta
(GMT+07:00) Krasnoyarsk
(GMT+08:00) Beijing, Chongqing, Hongkong, Urumqi
(GMT+08:00) Taipei
(GMT+08:00) Irkutsk, Ulaan Bataar
(GMT+08:00) Kuala Lumpur, Singapore
(GMT+08:00) Perth
(GMT+09:00) Osaka, Sapporo, Tokyo
(GMT+09:00) Seoul
(GMT+09:00) Yakutsk
(GMT+09:30) Adelaide
(GMT+09:30) Darwin
(GMT+10:00) Brisbane
(GMT+10:00) Canberra, Melbourne, Sydney
(GMT+10:00) Guam, Port Moresby
(GMT+10:00) Hobart
(GMT+10:00) Vladivostok
(GMT+11:00) Magadan, Solomon Is., New Caledonia
(GMT+12:00) Auckland, Wellington
(GMT+12:00) Fiji, Kamchatka, Marshall Is..
(GMT+13:00) Nuku'alofa

D

Technical Specifications

Technology	
Video Inputs (BNC)	1
Video Outputs (BNC)	1
Audio Inputs (RCA)	1 MIC-in port, 1 line-in port
NTSC/PAL	Auto-sensing or Manual
Network	
Protocols	TCP, UDP, HTTP, SMTP, FTP, NTP, DHCP, RTP, RTSP, DNS, DDNS, IGMP, UPnP, PPPoE and SNMP
Ethernet	Auto sensing 10/100 Mbps
Video	
Video Compression	MPEG4
Video Resolution	NTSC: Up to 30 frames at 176 x 120 Up to 30 frames at 352 x 240 Up to 10 frames at 640 x 480 or 704 x 480 PAL: Up to 25 frames at 176 x 144 Up to 25 frames at 352 x 288 Up to 8 frames at 640 x 480 or 704 x 576
Video Viewing	Adjustable image size and quality B/W or Color control Timestamp and text overlay
Serial Port	
COM port	1 (max. 115.2 Kbps)
Connectors	RS-232: Male DB9 RS-485: Terminal Block for Data +, Data -
GPIO	
Digital Input	2 (max. 12 VDC @ 50 mA)
Relay Output	2 (max. 24 VDC @ 1A, 125 VAC @ 0.5A)

LED Indicators	
PW1	Power 1
PW2	Power 2
FAULT	Power failure
VIDEO	Video communication active
AUDIO	Audio communication active
SERIAL	COM port status

Power	
Input	12 to 45 VDC
Consumption	7.5W

Mechanical	
Casing	IP30 protection, metal case
Dimensions (W x D x H)	53.6 x 135 x 105 mm (2.1 x 5.3 x 4.1 in.)
Weight	790 g
Installation	DIN-Rail or wall mounting

Environmental	
Operating Temperature	0 to 60°C (32 to 140°F) -40 to 75°C (-40 to 167°F) for -T models
Storage Temperature	-40 to 85°C (-40 to 185°F)
Ambient Relative Humidity	5 to 95% (non-condensing)

Regulatory Approvals	
Safety	CE, FCC
WARRANTY	5 years

Alarm Features

- Video Motion Detection with sensitivity
- Daily repeat timing schedule
- 3 color JPEG images for pre/trigger/post alarm image storage
- Automatic transfer of stored images via email or FTP with event-triggered actions

Security	User level password protection

Viewing System Requirements

- Internet Explorer 4.x or above
- Netscape Navigator 4.x or above

Software Bundled Free	
MOXA SoftDVR Lite	1- to 4-ch IP Surveillance Software for viewing & recording

E

Service Information

This appendix shows you how to contact Moxa for information about this and other products, and how to report problems.

In this appendix, we cover the following topics.

- **MOXA Internet Services**
- **Problem Report Form**
- **Product Return Procedure**

MOXA Internet Services

Customer satisfaction is our number one concern, and to ensure that customers receive the full benefit of our products, Moxa Internet Services has been set up to provide technical support, driver updates, product information, and user's manual updates.

The following services are provided

E-mail for technical support.....ventas@siesamx.com

World Wide Web (WWW) Site for product information:

.....www.siesamx.com

Problem Report Form

MOXA VPort 3310

Customer name:	
Company:	
Tel:	**Fax:**
Email:	**Date:**

1. **Moxa Product:** ☐ VPort 3310 ☐ VPort 3310-T
2. **Serial Number:** _____

Problem Description: Please describe the symptoms of the problem as clearly as possible, including any error messages you see. A clearly written description of the problem will allow us to reproduce the symptoms, and expedite the repair of your product.

Product Return Procedure

For product repair, exchange, or refund, the customer must:

- Provide evidence of original purchase.
- Obtain a Product Return Agreement (PRA) from the sales representative or dealer.
- Fill out the Problem Report Form (PRF). Include as much detail as possible for a shorter product repair time.
- Carefully pack the product in an anti-static package, and send it, pre-paid, to the dealer. The PRA should be visible on the outside of the package, and include a description of the problem, along with the return address and telephone number of a technical contact.

Soporte en Ingeniería y Equipos, S.A de C.V

¡SOLUCIONES!

Para el ahorro y control de la energía eléctrica

Calidad de la Energía Eléctrica
y Monitoreo de Parámetros Eléctricos
Bancos de capacitores.
Filtros de Armónicas.
Estudios de calidad de Energía.
Medidores de parametros eléctricos.
Protección para corrientes Transitorias.

AGUASCALIENTES (MATRIZ)

Priv. Cerro de la bufa No. 105
Fracc. Lomas del Campestre
Aguascalientes, Ags. C.P. 20129

Tel: (449) 145 6701
Fax:(449) 145 6703

GUADALAJARA

Siempre Viva No. 113
Col. Vista Hermosa
Tlaquepaque, Jal. C.P.
45615

Tel: (334) 624 2951

Toda la Republica

01 800 0877 783

ventas@siesamx.com